h e g

Haute école de gestion
Genève

How can distributed ledger technology systems accelerate the adoption of eHealth solutions by patients

Bachelor Project submitted for the degree of
Bachelor of Science HES in International Business Management

by

Camille RATTAZI

Bachelor Project Mentor:
John HERNIMAN, Doctoral Researcher at Cranfield University

Geneva, 21st August 2020
Haute école de gestion de Genève (HEG-GE)
International Business Management

Hes·so//GENÈVE
Haute Ecole Spécialisée
de Suisse occidentale

Disclaimer

This report is submitted as part of the final examination requirements of the Haute école de gestion de Genève, for the Bachelor of Science HES-SO in International Business Management. The use of any conclusions or recommendations made in or based upon this report, with no prejudice to their value, engages the responsibility neither of the author, nor the author's mentor, nor the jury members nor the HEG or any of its employees.

Acknowledgements

I would like to take the opportunity to share my gratitude to the following persons, who greatly supported me along the way and kindly shared their vast knowledge and expertise with me, which made this Bachelor thesis possible:

- First, Mr. John Herniman, to have always been available for long discussions and advice on key points, as well as to have provided exceptional guidance through the whole adventure of this project;
- Obviously, Mr. Francisco Diaz-Mitoma Jr., CEO and co-founder of Bowhead Health, based in Toronto, for having taken the time and energy on his busy schedule to be interviewed several times, to provide feedback to certain part of this thesis and to have greatly contributed by sharing his expertise of blockchain, his vision and company experience. But most importantly, for his collaboration and trust on the implementation of my survey in his mobile application;
- I am very grateful to all of the experts interviewed, including Alexis Roussel and Pierre-Mikael Legris for sharing with me their passion for data, health and distributed ledger systems, and for some of them, to have made the core of this thesis question possible;
- Finally, my sincerest thoughts go to my close ones for their kind words during this fastidious last year of studies, especially to Mr. Samy De La Fuente for his absolute day-to-day support, and particularly to Ms. Maylis Saiani for her unconditional encouragement and inspiration.

Executive Summary

This report’s goal is to understand how distributed ledger technology systems, especially blockchain, are beneficial in terms of eHealth adoption and patients control of their health data.

According to an executive in a multinational company of the health industry, “private data limits the growth of eHealth but also represent a better future. We must be inventive, or we will never get to revolutionize this industry”. It is a fact that personal data can be processed through blockchain systems as well as in a diverse range of processing operations (transfer assets, ensure traceability, or even to launch a smart contract). Many enterprises and governmental institutions are already using blockchain techniques and adoption of eHealth has been broadly covered. However, patient’s perspective on the use of blockchain in digital health solutions has not been empirically researched and thus does not have solid real-life implementations and understandings.

The analysis is based on empirical evidence from a group of 747 users of a live mobile application, Bowhead Health, which have utilised blockchain technology for developing solutions respecting user privacy and enabling considerable advances in the health industry; and from a broader online survey. Interviews of patients and experts in blockchain technology and health sector were also conducted.

By assembling the finding of the literature and the qualitative and quantitative research, it has been shown that: (1) even if a great majority of people do not understand DLT systems, they are still able to trust it, just like many other elements of our society (banks, lockers, HTTPS secured connection); (2) Blockchain associated with smart contracts appear as one of the most convincing solutions to provide informed consent, transparency and control, hence generating patients trust and establishing health data ownership at patient level. Moreover, patients have a tendency to overlook privacy concerns if their health data could help clinical research.

Ultimately, it is essential to simplify users’ understanding and ability to assess DLT by developing blockchain security indicators, facilitating the informed consent with user data flow control interfaces, as well as developing more partnerships with healthcare incumbents.

Consequently, this paper adds to literature by providing insights for the development of a healthy digital healthcare system that respects patients’ needs and rights, especially privacy.

Contents

List of Tables

List of Figures

Abbreviations and acronyms

AHT	:	Anonymized Healthcare Token
CAGR	:	Compound Annual Growth Rate
DHT	:	Digital Health Technology
DLT	:	Distributed Ledger Technology
EMR	:	Electronic Medical Record
GDPR	:	General Data Protection Regulation
HIPAA	:	Health Insurance Portability and Accountability Act
HCP	:	Healthcare Professionals (mostly physicians and pharmacists)
ICTs	:	Information and Communication Technologies
WHO	:	World Health Organization
eHealth	:	Digital Health
mHealth	:	Mobile Health

1. Introduction

1.1 Structure of the report

This report begins with providing a contextualisation of health, considering the unprecedented sanitary and political context in which the publication of this report takes place. Focusing on what digital health is, what it contains and what challenges it faces nowadays with regards to big data and privacy. It then clarifies the theoretical concepts related to the topic, learning what blockchain, consent and smart contracts are (Chapter 1).

Secondly, the current state of the art (Chapter 2) outlines what has already been written about the subject followed by the research gap that this paper intends to fill out. Further, the methodology part describes the approach chosen to conduct this research in terms of recruitment and data collection (Chapter 3).

Based on the exploratory work conducted, the later parts of this report analyse the data, summarize the results and present the findings (Chapter 4), by trying to answer to the research question and add to existing knowledge. The use of blockchain in digital health will be discussed (Chapter 5) and supported by a use-case, the Bowhead Health Inc. Canadian start-up and the key learnings behind their concept. Finally, based on the aggregated knowledge and findings, the conclusion delivers some recommendations and directions for future research (Chapter 6).

1.2 Health

Health is conceived as a global phenomenon, including physical, social and psychological dimensions. It is the foundation of an engaged and happy life, and modern humans have been the fortunate beneficiaries of great advances in medical technology (Collins, 2015). Humans have always been investing in health research, aiming to reach global health with the development of drugs, vaccines, diagnostics and other interventions against diseases such as malaria, cholera, pre-eclampsia, HIV and infectious diseases that represent public health challenges.

By definition, global health transcends borders. For this reason, health is a public matter and must be a collective, shared effort. To be effective, the healthcare system requires involvement and responses from additional sectors. *"We face shared threats and we have a shared responsibility to act."* (WHO, 2020) It requires nations, companies and individuals to act independently and in collaboration for general welfare.

In that sense, the World Health Organization reports in 2020, 13 urgent and often interlinked challenges for the next decade, such as : expanding access to medicines; stopping infectious diseases; elevating health in the climate debate; preparing for epidemics; investing in the people that defend our health; earning public trust; harnessing new technologies.

2. Literature review

2.1 Theoretical background

The global healthcare context has extremely evolved in 2020, clearly marked with what has been the worst global health crisis since 1918-1919[1], SARS-CoV-2[2], more commonly referred as COVID-19. The World Health Organization (WHO) declared the international health emergency on the 30th January 2020, activating a societal, economic and social slowdown of unprecedented scale. Since then, many countries took urgent decisions: China has taken a radical decision to quarantine the country, the entire security system of the communist regime has been converted into a health and social control apparatus; Italy put 15-millions of inhabitants in quarantine; Spain went through near-total isolation and many more countries followed with more or less strict actions. Worldwide, tests' availability increases and as per the WHO daily situation report of 31st July, the world counted *17'106'007 cases and 650'805 deaths*[3.]. Besides, as per these reports and despite the quarantine, we are currently seeing a proliferation in cases. The Spanish Medical Association lately alerted its authorities to step up vigilance to prevent the country, one of the most bereaved in Europe, from being overwhelmed by a new wave of the pandemic (Renata Brito, Joseph Wilson, 2020).

The current COVID-19 crisis highlights a number of successes and dysfunctions in our healthcare system. Even if the pandemic is not over yet, some lessons can be formulated out of it.

The use of technology and e-health highlights the very different levels of maturity in different countries, but one thing is clear: where technology is widely used, the consequences of this epidemic can be contained more quickly and effectively. In Germany, Israel, South Korea, Hong Kong and Taiwan, this involves the mobilization of technology, the use of health data, the use of multiple tests, including rapid testing to slow down the epidemic. (Institut Montaigne – eHealth report, 2020: 7)

It shifted priorities, mindset and trends. *"It accelerated work to improve health access and outcomes among people with complex health and social needs"* (Lauran Hardin, MSN, 2020). As human interactions are indispensable to provide the best care and technical

[1] «L'OMS ne sortira pas indemne de cette pandémie», 2020. Le Temps [online]. [Viewed 18 March 2020]. Available from: https://www.letemps.ch/monde/loms-ne-sortira-indemne-cette-pandemie

[2] severe acute respiratory syndrome coronavirus 2, discovered in 2019 in Wuhan (China) is a new strain of the coronavirus species SARSr-CoV.

[3] Coronavirus disease (COVID-19) Situation Report – 190 - 31st July 2020. [online]. [Viewed 1 August 2020]. Available from: https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200731-covid-19-sitrep-193.pdf?sfvrsn=42a0221d_4

efforts, most importantly in retail, food, manufacturing and logistics manufactures. In these times of social distancing, the situation also notably outlined the need and importance of: global collaboration, when 67% of adults rank global cooperation in health crises a top priority[4]; community spirit and reliable information.

Indeed, the rapid spread of the epidemic has been accompanied by false rumours and misinformation. Thus, there is an urgent need to strengthen the sources of accurate information, and to develop everyone's ability to assess its reliability. As an example, in some countries like Japan, even before the emergence of the coronavirus, the general public had difficulty accessing quality medical information due to a lack of central public organization in charge (Nakayama Kazuhiro, 2020).

The confidence factor was key for an optimal management and amelioration of the situation. Regular communications from the WHO, that manages and coordinates worldwide health-related activities, regarding the global evolution of the virus were vital to counter the false content circulating, mostly on the internet. 77% of the Americans trust the WHO as per a survey carried out in March 2020 by Morning Consult[5]. They trust it more than their own government and army.

Furthermore, the quarantine has forced people, workers, companies and universities to adapt and invest in remote work and distance learning. Nationwide closures impacted over 60% of the world’s student population (UNESCO, 2020). As a result, remote technologies and digital solutions have grown significantly, implemented with virtual reality, augmented reality, 3D printing and artificial intelligence. More and more users converted to online shopping, virtual meetings, cloud technology, work collaboration tools and contactless payment methods have spread. The business world testified the development of 3D printing that reshaped supply chain by reducing surprises and increasing flexibility, in a period of shortage of essential life-saving devices. Telehealth, which includes preventative, promotive, and curative care delivery delivered by information and telecommunication technologies (Health Resources and Services Administration, 2019) has greatly gained in popularity in rural settings as well as in big cities and is here to stay. Coronavirus offered the most efficient and rapid boost in telehealth that many were waiting for for years.

On the market side, global spending in health is expected to increase to $18.28 trillion worldwide by 2040 (Institute for Health Metrics and Evaluation, 2016) as more public health

[4] (Morning Consult, 2020: 10)

[5] (Morning Consult, 2020: 3)

challenges arise. Shifting in trends contribute to the growth of the investment in home healthcare market. Indeed, as per a recent report from Grandview Research Inc. (2020), its global size is anticipated to reach USD 515.6 billion by 2027, with a compound annual growth rate of 7.9%, compared to 281.8 billion in 2019.

The context of unprecedented health crisis linked to the Covid-19 pandemic has shown the ability of all health actors to innovate together and has certainly precipitated the adoption of eHealth solutions.

2.1.1 eHealth

By definition, digital health, more commonly called eHealth, is the term used to describe all electronic health services, in which information and communication technologies (ICTs) are used to improve the processes of the health system and to network the actors involved.[6]

Technologies comprised in the word eHealth are various and aim to answers to several needs notably in the field of prevention of diseases and symptoms in general, in the area of chronic illnesses by monitoring, alerting, assisting in defining causing factors, and facilitating the treatment process. These tools have not only transformed millions' daily lives, traditional services and business models but it has also empowered populations in almost every area of the economy. Healthcare will be no exception.

Digitalization of the health system brings up a large number of benefits including patient empowerment, telemedicine, dematerialization of exchanges, process improvement (for example, help with patient volume management on-field), digital tools, artificial intelligence as well as automation. The promise of *"digital health technology (DHT) is to support self-management by enhancing the sense of control patients possess over their disease".* (Patrick Slevin, Threase Kessie et al., 2019: 1)

Four general domains can be identified in digital health technology: Telehealth; Mobile health (mHealth); Digital health systems; and Health Analytics. Components can be hardware, software or service.

- Telehealth is the broad term that refers to remote health services, not involving direct clinical services like diagnosis, treatment, or care to the patient but targeting the improvement of the healthcare delivery as a whole (Samaranayake, 2020). As per UKTelehealthcare (2017), these services offer independence, since the patient can self-manage its condition by entering data or having the "data collected by various

[6] (my translation of eHealth Suisse, 2017)

devices (blood pressures readers, pulse oximeters, and blood glucose monitors) which automatically transmits the readings“ to a monitoring service for potential alerts to be sent. This domain is not to be mixed with Telemedicine, that has spread during the quarantine, which is a subfield of telehealth and allows professionals to provide direct clinical health care services, by using video technology and software to diagnose and treat patients remotely.

- In addition, Telehealth and telemedicine are also not to be mixed with Telecare, another branch that initially provides remote care to vulnerable people or elderly. This involves continuous and automatic activity monitoring for vital health parameters with environmental and personal sensors, for instance: flood detectors, fall detectors, medication reminders.[7] Telehealth often includes mobile health devices to monitor and deliver care, for instance with mobile apps offering teleconsultation.

- Mobile health (mHealth), “is the use of mobile technologies to support health information and medical practices” (Peterson et al., 2016). They include: Wearables such as glucose meter, pulse oximeter and sleep monitors; and Apps, such as medical apps (for appointments and reminders) and Fitness apps (Fitbit, Nike Run).

- Digital health systems aim to dematerialize data and facilitate exchange of information between the actors, they consist of E-prescribing systems, Electronic health records (EHR) and data-sharing tools.

- Health analytics is the way of transforming data into actions by providing insights for fact-based decision making in healthcare (Simpao et al., 2014). It includes “data mining, text mining, and big data analytics” (Islam et al., 2018), to control the spread of a virus or to decrease hospitals readmission rates for instance.

Please note that digital technologies in general may have more than one specifc intended use. Due to the constantly evolving nature of this technological environment, this list is non-exhaustive and subject to change, but provides a global outline of the current available technologies and tools.

Without a deep understanding and knowledge of the functioning, ethics and societal impact of the eHealth technologies above, they could rapidly turn harmful to the people they aim to care for, by not sufficiently protecting their data for example. It is important to understand that health is one of the least digitalized sectors of the economy but also one of the most

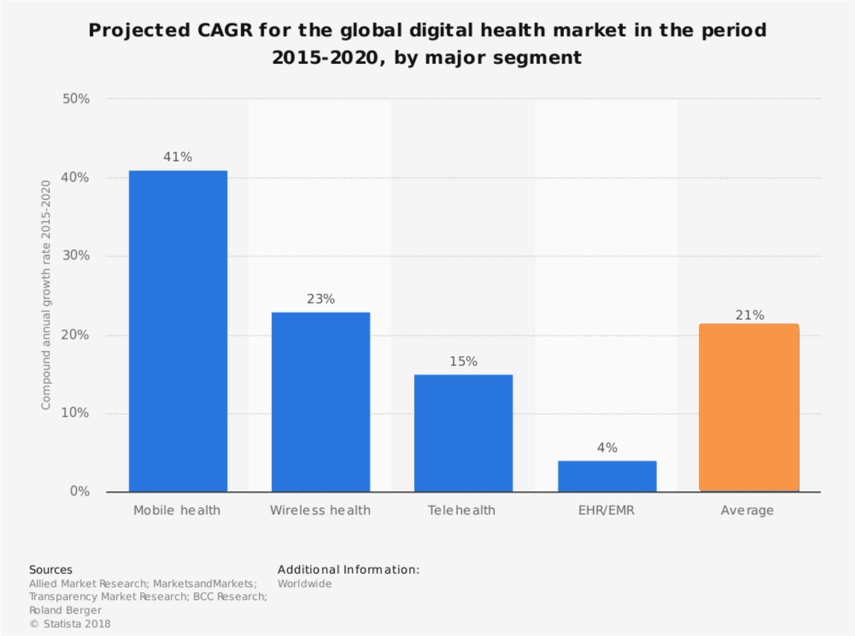
[7] (UKTelehealthcare, 2017)

complex and sensitive one to transform, due to the number of data and actors it involves. With regards to the rapid expansion of those technologies in the last decade and especially in the past few months, monitoring and regulation of eHealth is critical and represents a global challenge for health care actors, physicians and regulators. Very well aware of the new issues and challenges it implies, The World Health Organization (WHO) even created a global multi-disciplinary technical group in 2019 to provide guidance and address matters related to digital health.

With the coronavirus crisis, increasing demands for telecommunications technologies have fertilized the industry for the launches of new tools and services. Simultaneously, the strict regulations imposed by the governments to mitigate the virus spread are supporting the industry growth by boosting health analytics, "*used to track the spread of COVID-19 infection, to optimize the usage of hospital resources and triage of the patients for treatment*" (Sumant Ugalmugle, 2020).

The market

Figure 1 - Projected CAGR for the global digital health market, 2015-2020, by major segment

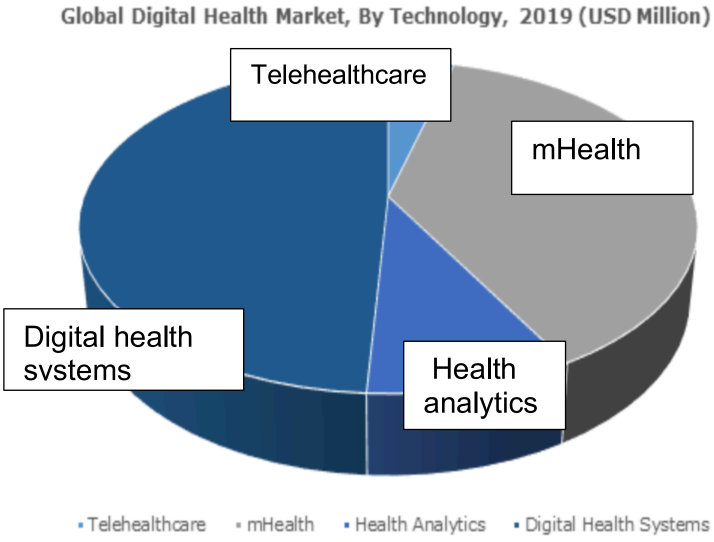


Source: Statista, 2018

As per the graph above, in 2018 already, the digital health market was forecasted to reach over 200 billion U.S. dollars by 2020. Driven particularly by the mobile health market with a compound annual growth rate (CAGR) of around 41 percent." The average CAGR of the digital health market stands at 21%. (Statista Research Department, 2016).

“After three consecutive years of growth, venture deals, and dollars for digital health companies declined in 2019”, said Raj Prabhu, CEO of Mercom Capital Group. The numbers include Social Health, Mobile Health (mHealth), Telehealth, Personal Health, Rating & Shopping, Health Information Management, Revenue Cycle Management, Service Providers and Security. These figures clearly show a slowdown in investment and interest from investors that is expected to significantly regain in interest with the largescale health events of 2020.

Table 1 - Global Digital Health market structure by technology in 2019



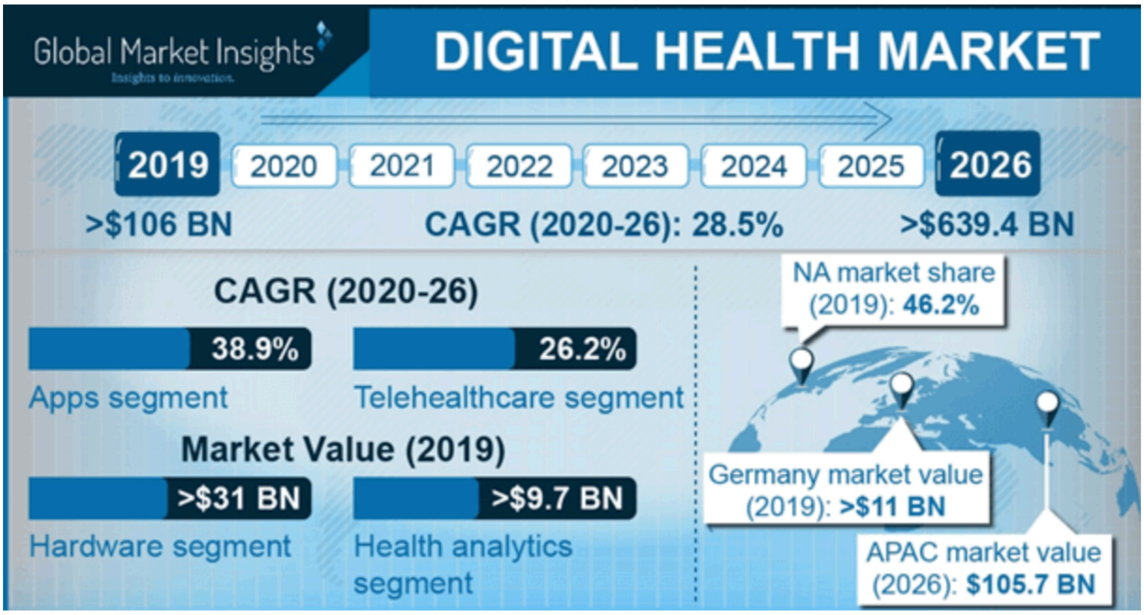
Source: Global Market Insights, 2019

The table above pictures the USD 106.3 billion global digital health market and its composition in 2019 (Global Market Insights, 2019). Mobile Health (mHealth) and digital health systems stand covering the major part of the market. Telehealth being the smallest part of the pie at the time. Besides, “the European market was valued at nearly USD 37 billion in 2019” a significant part of the global industry. (Sumant Ugalmugle, 2020).

Nevertheless, with the current perspective of the sanitary crisis, health analytics, mobile applications and telehealth are expected to demonstrate an unprecedent growth, supported by governments’ anti COVID-19 initiatives and growing start-ups market penetration.

As a result, the “Digital Health Market size is projected to exceed USD 639.4 billion by 2026”; according to a new research report by Global Market Insights, Inc. below.

Figure 2 - Digital health market, 2020-2026 projection



Source: Global Market Insights, 2020

In addition, the CAGR standing for Compound Annual Growth Rate, is estimated to 28.5% for the sixth coming years, showing a high growth compared to the different predictions made in the past.

In terms of investment, as per Mercom Capital Group, the top highest-fund global digital health categories in 2019 were Telemedicine ($1.76 billion); Health Analytics ($1.64 billion); Mobile health apps ($1.23 billion). This year, a significant boom was witnessed in venture capital investment for digital health start-ups in the first 2020 quarter (Sumant Ugalmugle, 2020).

For all of these reasons and promising figures, digital health is a trendy, prosperous and promising market of high complexity. Yet, due to the large scale and such rapid adoption, broadly accentuated by the confinement of populations this year, concerns of privacy and data leakages quickly arose as seen with teleconference tools like Zoom's and its vulnerability to cameras hijacking and personal data breaches.

2.1.1.1 Challenges

More than ever, the large-scale actors, healthcare providers, technology firms, start-ups, hospitals and pharmaceutical companies on the market need to quickly integrate digital solutions to adapt to this ever-changing environment. However, implementing such processes requires a massive amount of data and brings up numerous challenges, including data standardization, patient understanding and most importantly patient data security. There are numerous barriers to the development of digital health, including:

- no complete use of health data due to its complexity, mostly to insufficient investment in information systems and their management;
- lack of specific training and equipment for HCPs;
- lack of patient awareness on the possible solutions;
- a heterogeneous and poorly structured health care sector;
- a creation framework of infrastructures and new technologies that does not sufficiently involve patients
- insufficient incentives towards telehealth solutions in the past, although this issue has been greatly taking care of and boosted by the current sanitary crisis;
- Lack of data mostly because of a global lack of trust, knowledge in information systems;
- Uneven access to technology

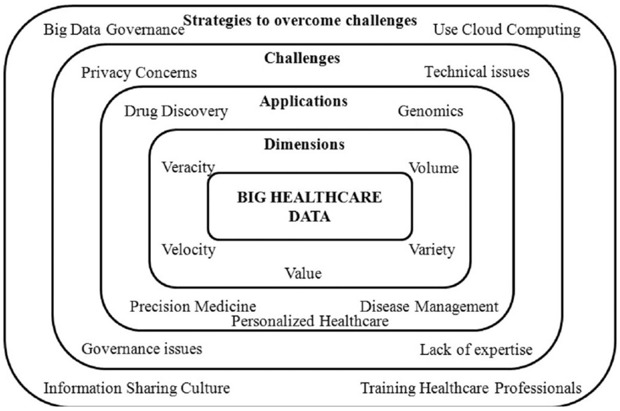
These issues were confirmed by Olaronke et al. (2016), which study "revealed that the fragmentation of healthcare data, ethical issues, usability issues as well as security and privacy issues are some of the factors impeding the successful implementation of big data in healthcare".

2.1.1.1.1 *Need for data*

An article by Li et al. (2016) found on Google Scholar, outlines the lack of data on the healthcare market that prevent newly established healthcare facilities to "*build a robust decision-making system due to the lack of sufficient patient records. However, to make effective decisions from clinical data, it is indispensable to have large amounts of data to train the decision models".* Li also highlights that there are conflicts of objectives between "preserving patient privacy and having sufficient data for modelling and decision making". This implies that actors have to face a double constraint: the need for patient health data to develop proper personalized eHealth technologies, simultaneously with a data shortage due to the privacy constraint laws foster.

On the other hand, "the vast volume as well as the complexity of these data makes it difficult for the data to be processed and analyzed by traditional approaches and techniques" (Olaronke et al., 2016).

Table 2 - Healthcare data at the core of the healthcare ecosystem



Source: Mehta and Pandit, 2018

As shown by the Table above, big data are key since they are the core of the healthcare ecosystem, bringing dimensions, opportunities and challenges to table, such as privacy concerns and technical issues.

2.1.1.1.2 Leakages

Internet data has become so hazardous and data theft so common that trust in the companies supposed to protect data has been weakened.

In the United States, as per the Identity Theft Resource Center, the total number of breaches reported in 2019 is up by 17% since 2018 (ITRC Data Breach report, 2019 : 2). The Medical and Healthcare sector sits at the second place, right after the Banking/Credit/Financial sector in terms of sensitive records breaches with a total of 39 million (39'378'157) sensitive records exposed. 35.64% of the total security breaches came from Medical/Healthcare. This is extremely concerning knowing most of the data in healthcare are often personal health information, and thus, extremely sensitive.

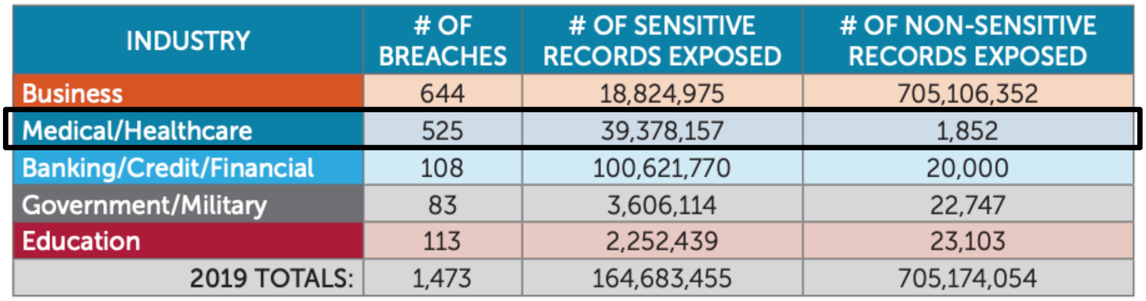
In fall 2019, the largest medical testing company in Canada, Lifelabs, was hit by a ransomware attack on their servers. 15 million of Canadians have seen their data stolen, including their genomic records[8], the very core of our being. They are accused of not having implemented good procedures and having conducted inadequate security policies for the safety of their patients' information.

That same year, "American Medical collection Agency (in its entirety) *database had been found for sale on the dark web that included information from 27 separate entities, including*

[8] From modern biology, Genomics is the science of genomes: it studies the DNA sequences of living beings. Given the large amount of data, genomics uses bioinformatics to store and analyze information.

AMCA. Information such as names, payment card information, name of lab or medical service provider, date of medical service, referring doctor, some medical information, Social Security numbers and contact information was exposed." (ITRC Data Breach report, 2019: 9).

Table 3 - 2019 Summaries of breaches in the United States per industry



INDUSTRY	# OF BREACHES	# OF SENSITIVE RECORDS EXPOSED	# OF NON-SENSITIVE RECORDS EXPOSED
Business	644	18,824,975	705,106,352
Medical/Healthcare	525	39,378,157	1,852
Banking/Credit/Financial	108	100,621,770	20,000
Government/Military	83	3,606,114	22,747
Education	113	2,252,439	23,103
2019 TOTALS:	1,473	164,683,455	705,174,054

Source: ITRC Data Breach report, 2019

In 2019, there was around 29 million more cases of sensitive health data exposed than in 2018. In the European Union, as regulations on data privacy and cybersecurity are stronger, the total breaches reported since May 2018 are 160'000. In the Medical and Healthcare sector, the most used method is Unauthorized access (when somebody manage to get access to a program, website, server or device using someone else's account without their authorisation) followed closely by Hacking/Intrusion. Employee negligence also figures in the top 3 methods. Most recently, on July 21, 2020, Doctolib's online appointment scheduling service was attacked from a patient account. The attacker was able to exploit a vulnerability in the web application's code that allowed him to illegally access approximately 6,000 patient appointments by sending random requests. These parameters were then transferred to Doctolib's backup database by the link editor (third-party program) under the responsibility of the healthcare institution (Portail d'Accompagnement Cybersécurité des Structures de Santé, 2020). Systems for reporting similar serious safety incidents have been put in place, particularly in Europe, for instance in 2017 in France, obliging healthcare players to inform their regional health subsidiary of these major incidents.

Obviously, these events were only some of the latest examples of the innumerable data breaches happening every year, not to say every month. The consequences of such leakages are heavy and extremely costly, for the patients as well as for the company whose servers are being hijacked and subject to ransom demands. As a consequence, it is the entire health organization that has to restructure its brand image, suspend its medical activity until the issue is solved, losing their patients' trust on the way. Hence, the main challenge for the digital health industry - one of the most affected by cybercrime - here is to foster a safe environment protecting the patient information at all costs. The challenge that such demand for privacy incurs is significant.

2.1.1.1.1 Privacy

First, data security not only allows one's protection of credit card details, locations or medical records, it gives privacy. But what really is privacy? Privacy is a human right that protects one's private life, communications, and ability to choose what content and actions to share with others. It allows to maintain boundaries between people, to ensure one's control over his information and to decide whether or not to withdraw personal data barriers. At the end of the day, privacy is power, the more one has it, the more control one has on his daily life. At the same time, it is not always about the information that are intentionally given or posted. In fact, users have very little control or knowledge about what information is being immitted from their digital devices, smartphones, laptops or connected tools.

> *« The invention and public adoption of computers forced an expansion in the understanding of privacy to include a right to the protection of personal information. Accordingly, in 1971, the German State of Hessen adopted the world's first data protection law to regulate the conditions under which public and private actors could handle individuals' personal information. »*
>
> (Unicef Children's Rights and Business in a Digital World)

After 1971, the related regulations baseline evolved, in the US, it is the Health Insurance Portability and Accountability Act (HIPAA) of 1996 that is in force, while in Asia data privacy laws are fragmented, Japan is making efforts, but Chinese's personal data protection is not protected by a specific law even though their government was the first to gather massive amounts of data during the pandemic. The General Data Protection Regulation (GDPR) of April 2016 applies for all European member states and often serves as a foundation for drawing data privacy laws outside Europe. These regulations' goal is to harmonize data privacy laws and set a general framework across their respective countries by creating administrative, physical and technical safeguards.

The convenience of new technologies and poor management have occurred massive leakages. New laws and regulations have thus come into force to face these new threats. "Around 100 countries now have some form of privacy and data protection law" as per Privacy International (2017). Governments are aware of the issues and most of them are taking actions. As per a report by the WHO, 70% of their Member States already implemented a national e-Health policy or strategy in their territory (World Health Organization, 2016: 7), showing a high involvement and considerable public investments from government to regulate and support this emerging domain.

The development of e-health brings many challenges in terms of supervision and protection. There are many regulatory issues at stake, affecting medical institutions, European and governmental bodies, practitioners and patients. It is important to provide a framework for health innovations by systematically considering the constraints and uses of these new health practices. As long as a legal vacuum accompanies these new technologies, their use will be relatively inefficient. Indeed, research tends to show that *"more than 40% of users no longer use them passed a trial period of approximately 3 to 6 months"* (Beatty et al. 2013 quoted in Del Rio Carral et al., 2016 : 31). As per Del Rio Carral et al. (2016), this abandonment rate could be due to poor management and fear of data appropriation, which may be the cause of the lack of acceptance of these technologies.

But are people ready to sacrifice a part of their health data privacy to reach personalized healthcare? According to a study on medical secrecy with regards to new technologies by Miquet-Marty et al. (2018), the points of view of the general public and doctors were analyzed. The results show that for both groups interviewed, for 58% of the general public and 66% of doctors, with the development of new technologies in the health sector, medical secrecy "will be more difficult to respect than before, because personal data will never really be secure", followed by 23% and 24% who believe that it will be neither more difficult or easier. Very few believed it could help data getting safer.

Boulos (2014) concluded that apps could create "*additional risks for less experienced users who might find themselves tricked to download apps that contain malware, or violate their online privacy"* and thus recommend educating patients on the potential dangers, because as stated : "The best first line of defence was, is, and will always be to educate consumers."

Although the processing and use of this data falls within a legal framework that draws its sources from different legislations, e-health is not rooted in every jurisdiction. Thus, the sharing of medical data would make it possible to improve patient care, but the danger of its collection by third parties represents a major obstacle. (Editions legislatives, 2018).

Healthcare data generated by wearables and other digital health devices could generate tons of insights and value for patients, but this promise could be hampered by concerns of data mismanagement and privacy. Assuring people of their data protection and privacy as well as protecting them from leakages and mismanagement remain crucial in the development of new tools. These concerns could be mitigated by establishing the right decentralized technologies and instituting proper legal framework.

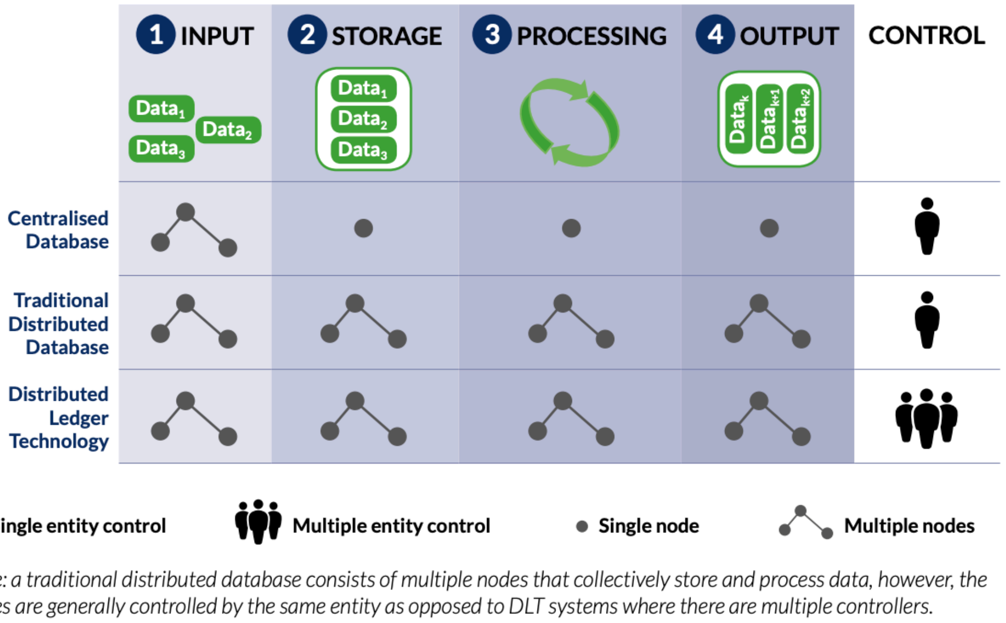
2.1.2 Distributed ledger technology

Distributed ledger technology (DLT) is the technology behind decentralized network, and thus, behind blockchain, introduced by Bitcoin in 2008. There are a “multitude of conflicting definitions” to what distributed ledger or blockchains are and consist of. Many of the most common, well-rooted and precise definitions of them have brought confusion by excluding many potential applications of these technologies (Michel Rauchs, 2018: 21). For this reason, this report will define distributed ledger technology (DLT) systems as depicted by The University of Cambridge in their 2018 Conceptual Framework report. DLT system is a *“consensus machine: a multi-party system in which participants reach agreement over a set of shared data and its validity, in the absence of a central coordinator”.*

2.1.2.1 *Decentralization*

When a database or network is decentralized, it means that partitions of the database can be divided and managed by different group of persons with different needs (for instance different departments in a company). It is also spread across different storage device locations to increase its security and flexibility. Still, the management of such distributed databases is complex and challenging to maintain. It differs from centralized database for example, which data are accessible in its entirety and located at one specific storage device.

Table 4 - From Centralised databases to Distributed Ledgers



	1 INPUT	2 STORAGE	3 PROCESSING	4 OUTPUT	CONTROL
	Data$_1$ Data$_2$ Data$_3$	Data$_1$ Data$_2$ Data$_3$	↻	Data$_k$ Data$_{k+1}$ Data$_{k+2}$	
Centralised Database	∧	●	●	●	👤
Traditional Distributed Database	∧	∧	∧	∧	👤
Distributed Ledger Technology	∧	∧	∧	∧	👥

👤 Single entity control 👥 Multiple entity control ● Single node ∧ Multiple nodes

Note: a traditional distributed database consists of multiple nodes that collectively store and process data, however, the nodes are generally controlled by the same entity as opposed to DLT systems where there are multiple controllers.

Source: Rauchs et al, 2018: 23

As pictured by the table above, what distinguishes a DLT system from a centralised database is the multiple nodes[9] possibilities in storage places, processing and output, as well as control opportunities. Then, what differs DLT from standard distributed database is the fact that it can be used in various hostile environments, experiencing high adversity and with various actors (controllers).

- Distributed: stands for Decentralized
- Ledgers: are databases of transactions grouped into records
- Technology: stands for the protocol enabling the execution of such a database in a decentralized way, removing the need for a central authority to control the operations (Jake Frankenfield, 2018).

As per Frankenfield (2018), many companies already keep their data at different locations. However, these locations are often linked to a central database. The latter is then vulnerable to cyber-crime and delays, since each one has to be handled and updated distantly.

DLT, on the other hand, its "*very nature of [a] decentralized ledger makes them immune to a cyber-crime, as all the copies stored across the network need to be attacked at the same time for the attack to be successful. Additionally, the simultaneous (peer-to-peer) sharing and updating of records make the whole process much faster, more effective, and cheaper" (Jake Frankenfield, 2018*). So, the security of a decentralized system is easier to maintain and since data are spread, less information is accessible at each touchpoint. Knowing the vulnerability of the health system, the association of this technology with one of the most cyberattacked industry, appears now to be logical and very valuable.

2.1.2.2 *What is a blockchain?*

By definition, blockchain is defined as a type of distributed ledger. It consists of a digitized ledger or database for storing information, which keeps track of all of the history of "blocks" of information. Blockchains are computer technologies that organize trust in the recording, transmission and storage of transactions. As it is distributed, they are not subject to the control of any central entity.

Appeared in 2018, it is a decentralized, transparent and reliable agent. *"It allows for the transfer of ownership of units using an encryption system without requiring control by the government or a central bank"* (Joshua Esan, 2020).

[9] Node: a data point of connection linked to several other data *points, « a place where things such as lines or systems join (Cambridge Dictionary).*

There are two kinds of blockchain, private and public. Private blockchain, or "permitted" blockchain, is a kind of distributed ledger *"whose content is not publicly available and/or whose validation is subject to pre-established permissions by an authority"* (Frederic Lars, 2018). Meaning that one has to be granted access to use it. Nevertheless, since the blockchain technology used in this report's use-case is public, the private blockchain will not be covered in this report.

On the other hand, a public blockchain is an anonymous channel that is both visible and modifiable in a public way by everyone. Among the public blockchains are notably:

- Bitcoin: the first and most important public blockchain born in 2008;
- Monero: a special public blockchain, since it contains unreadable transactions, so that Monero (XMR) is considered an anonymous crypto money.
- Ethereum: a smart contracts platform whose operations are stored on a public blockchain validated by Monero. As per Ethereum themselves (2020), *"It's the world's programmable blockchain"*[10]*.*

This latter is the public blockchain referred to when writing about blockchain in this project, since it is the one used by the mobile application Bowhead Health, which will further be presented as one of the innovative real-life implementations of blockchain use for digital health purpose.

The deployment potential of the blockchain is such that it moves away from its original purpose of digital money. Since it removes the necessity of trusted third-party it opens the door to a lot of implementations' possibilities (finance, health, transport, insurance, real estate). Comparable to a "big ledger in which everyone can write […] but nobody can delete, falsify or destroy any lines" (my translation of Comtesse, 2017). For these reasons, it can meet the demands for greater transparency and confidence in health data. DLT systems such as blockchain platforms should allow for better data management and security, as it will be impossible to change the recorded data, for instance patient consent, medical documents, drug supply chain and clinical trials information, without risking a break in the blockchain because of the core of its design. An altered block in the blockchain is immediately recognizable and thus, informs the actors of the alteration of the data.

[10] What is Ethereum?, [no date]. ethereum.org [online]. [Viewed 12 August 2020]. Available from: https://ethereum.org

2.1.2.2.1 What are smart contracts?

Smart contracts are a concept that freezes and captures an arrangement between two people in a blockchain in the form of an algorithm. They allow the exchange of all kinds of assets, money, goods or services without the use of intermediaries. Basically, they are self-executing contracts programs that control the transfer of digital currency or assets between parties under specific conditions. Thus they automate the exchange of value in the form of cryptoactives and make it possible to add specific conditions to these exchanges.

Hence, the initial aim was to provide an alternative to the current financial system thanks to the blockchain technology and the decentralization, the obligation linked to the contract is therefore guaranteed by a computer code, and no longer by law. This has proved that it is possible to exchange and contract without intermediaries, such as banks or notaries for example.

How a smart contract works : the smart contract is a digital version of the traditional paper contracts. During the execution of one of the latter, all the validation steps are recorded in the blockchain used, most often Ethereum, which makes it possible to secure all the data and a modification or deletion of the latter afterwards (Floriane Bobée, 2019).

Here are some of the advantages linked to smart contracts:

1) Accuracy: Unlike traditional contracts, smart contracts are extremely accurate. With them, all the conditions governing the contract are explicitly recorded. Indeed, the lack or omission of a term in a contract can lead to numerous procedural and implementation problems. The smart contract aims to reduce or even make such errors impossible in the future.

2) The transparency aspect: The terms and conditions of smart contracts are of course visible and accessible to all stakeholders involved in the contract. Once the terms and conditions have been established, nothing can be changed. This obliges all the parties involved in the contract to be totally transparent in their dealings with the contract.

3) Speed: the processes are almost instantaneous. When the conditions are met, the contract is validated. Smart contracts make the use of paper-based contracts totally useless and obsolete. This is also good for the environment.

4) Security: the use of smart contracts coupled with blockchain technology makes it impossible to manipulate, falsify or make mistakes as with traditional contracts. The fact that smart contracts are totally autonomous and transparent, allows its users to have great

confidence in this system. Once the contracts have been validated and executed, they remain forever present and can be consulted on the blockchain.

5) Reduction of costs: Smarts contracts eliminate a very large part of intermediaries such as bankers, lawyers or notaries for example. This makes this technology and the execution process much cheaper and more efficient. The fees due to these intermediaries are no longer applicable.

Equally, like any computer system, it has some disadvantages, the main one being the risk of miscarriage and breaches. The code of the latter being most often open source, if it is badly realized, it could allow malicious people to slip into the rift and exploit the data to the detriment of users. Moreover, it is worth noting that as the complexity of the contract increases, the risk of creating a coding flaw increases.

2.2 Specific literature review

The previous external sources of literature offered theoretical foundations to this report. This section narrows down to the Digital health literature directly related to the research question, hence reviewing the existing documents on the implementation of DLT systems in eHealth and their adoption by patients.

2.2.1 Digital Health

As McKinsey article on the Healthcare's digital future highlighted, "the healthcare industry is on the cusp of a third wave of IT adoption", encouraging actors to engage massively in all of the digital health technologies (McKinsey, 2014).

Indeed, according to the study carried out by Velin Stroetmann et al. in 2007, "eHealth for safety", solutions based on eHealth or information and communication technology (ICT) were already considered as essential tools to meet health challenges in the future. In this study, the authors identify the potential benefits created by the use of ICT and show that new health technologies not only help to reduce the rate of errors in care by providing more accurate and transparent information, but also by facilitating a rapid response to an adverse event, improving diagnosis and treatment with relevant decision support as well as monitoring and feedback on these events. e-Health helps to retrieve and aggregate citizens' health information and thus to make prevention and care more effective, especially for the management of chronic or long-term diseases (Stroetmann et al., 2007).

Many reports and articles relate the use of digital health technology in mental illnesses11, management of pain12, weight control13 and impact on traditional healthcare culture14. From BERTALAN et al. (2017) patients' change of role, shifting "from being a passive stakeholder of care to becoming proactive", to the need for evidence base demonstrating the *"effectiveness of these technologies in improving the outcomes in larger patient populations"* (BATRA et al., 2017), all of them conclude by showing the benefits of DHT in healthcare, hence confirming Velin Stroetmann research in 2017.

At the same time, mHealth literature is widespread. Mobile health and wearables personalized for people, represent a great potential and opportunities for the improvement of care. In 2017, the French eHealth Alliance mandated by the State, called for the

11 (BATRA et al., 2017)

12 (BHATTARAI and PHILLIPS, 2017)

13 (THOMAS, J. and BOND, D., 2014)

14 (BERTALAN et al., 2017)

implementation of a labelling repository for connected Objects and mobile health applications. They reminded that “making full use of these technologies implies creating the conditions for trust by their users” (my translation of Jocelyne M., Ministère des Solidarités et de la Santé, 2017). Indeed, a repository could be a great idea to mitigate the risk of poorly designed applications, as raised by Boulos et al. (2014) who questioned the reliability of “*unregulated medical apps”.*

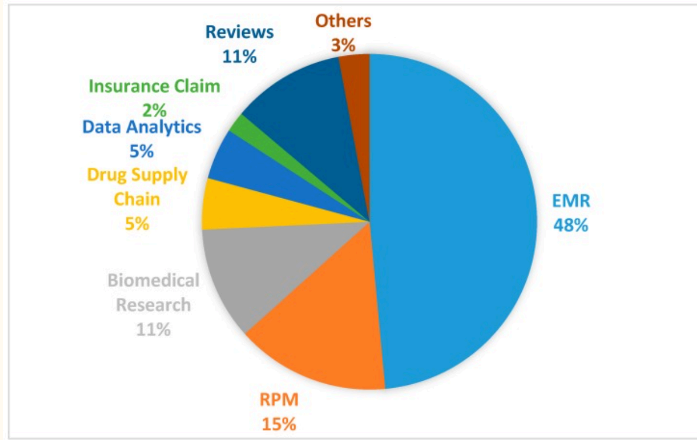
Lastly, as per Latulippe et al. (2017) in their Social Health inequalities and eHealth report, one of the most present dangers of e-health applications lies in the misuse of collected data in purposes other than those originally intended, a huge social, but also economic and health gap could widen between users. If these sensitive data are subject to biased uses, then it is possible that important health authorities will exacerbate existing inequalities in care, based on the pace and lifestyle, but also on the socio-economic status of patients. Moreover, the very digitalisation of the health service is already causing a social divide. Inequalities in access to the Internet and to technologies affect patients' access to e-health. On the other hand, for users who live in rural or poorly accessible areas, but whose access to technology is not compromised, the use of ICTs represents a real improvement in access to care and health (Latulippe et al., 2017).

2.2.2 Blockchain in healthcare

As introduced by Cornelius C. Agbo et al. in his Blockchain Technology in Healthcare systematic review in 2019, “since blockchain was introduced through Bitcoin, research has been ongoing to extend its applications to non-financial use cases.” The health industry being one of the most promising field. When searching for literature on Google Scholar with “distributed ledger technology” as keywords, one can find that the actual literature for DLT is very rich and broad. The results found many recent studies for governments usage[15] to pioneering implementations in digital governments, to financial, manufacturing, energy, to retail. When looking for “blockchain in healthcare”, Google Scholar provides 23’000 of many applications and use cases.

[15] (Ølnes et al. 2017)

Table 5 - Percentage repartition of the papers, from "Blockchain Technology in Healthcare"



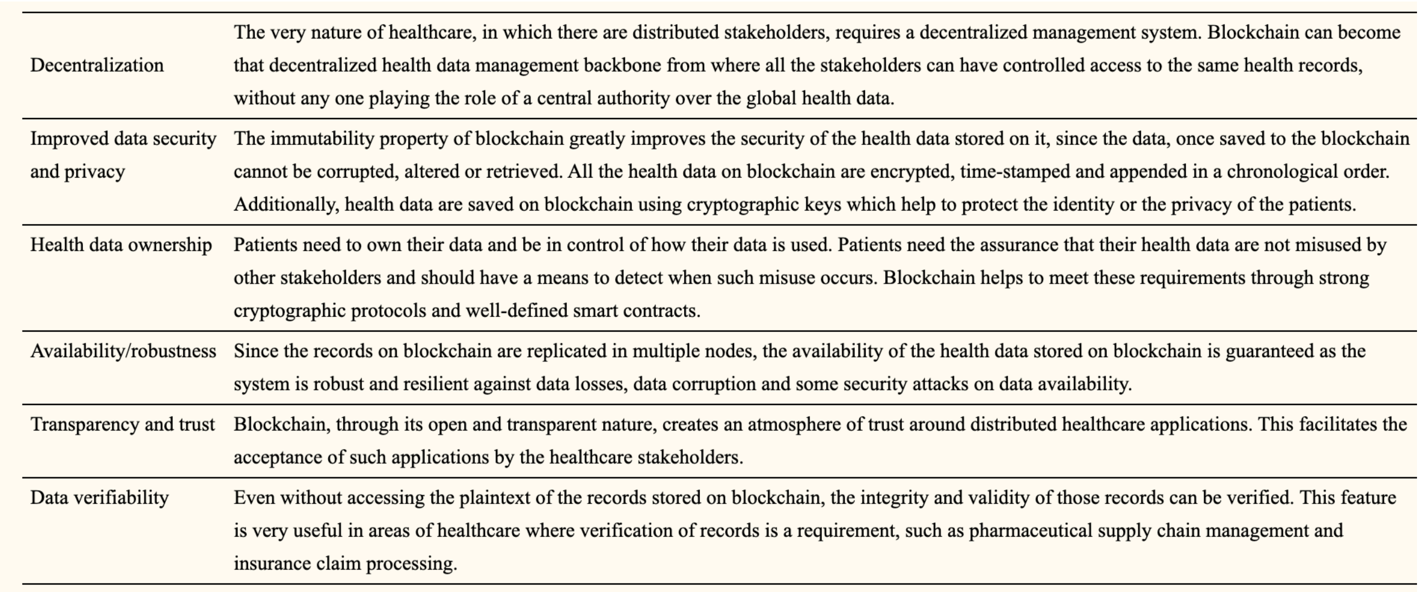
Source: Cornelius C. Agbo et al., 2019.

In their systematic review of the literature of blockchain in healthcare, Cornelius C. Agbo et al., (2019) gathered and analysed an enormous quantity of papers and selected 65 of them. The pie chart above is the percentage distribution of the selected papers, which is very representative of the current state of the art situation of blockchain's use cases in healthcare. Electronic medical record (EMR) being the most studied and represented in researches at the moment, due to the many ongoing governmental discussions around the subject[16]. This very relevant study from Cornelius C. Agbo et al. (2019), shows that 23 countries have issued papers on this subject which indicates that the "application of blockchain in healthcare is gaining global interest".

The main benefits are highlighted by the authors in the figure below, including the very notions of decentralization, improved data security and privacy, health data ownership, transparency and trust as well as data verifiability.

[16] (Leslie, Rock, [no date])

Table 6 - Benefits of blockchain to healthcare applications



Decentralization	The very nature of healthcare, in which there are distributed stakeholders, requires a decentralized management system. Blockchain can become that decentralized health data management backbone from where all the stakeholders can have controlled access to the same health records, without any one playing the role of a central authority over the global health data.
Improved data security and privacy	The immutability property of blockchain greatly improves the security of the health data stored on it, since the data, once saved to the blockchain cannot be corrupted, altered or retrieved. All the health data on blockchain are encrypted, time-stamped and appended in a chronological order. Additionally, health data are saved on blockchain using cryptographic keys which help to protect the identity or the privacy of the patients.
Health data ownership	Patients need to own their data and be in control of how their data is used. Patients need the assurance that their health data are not misused by other stakeholders and should have a means to detect when such misuse occurs. Blockchain helps to meet these requirements through strong cryptographic protocols and well-defined smart contracts.
Availability/robustness	Since the records on blockchain are replicated in multiple nodes, the availability of the health data stored on blockchain is guaranteed as the system is robust and resilient against data losses, data corruption and some security attacks on data availability.
Transparency and trust	Blockchain, through its open and transparent nature, creates an atmosphere of trust around distributed healthcare applications. This facilitates the acceptance of such applications by the healthcare stakeholders.
Data verifiability	Even without accessing the plaintext of the records stored on blockchain, the integrity and validity of those records can be verified. This feature is very useful in areas of healthcare where verification of records is a requirement, such as pharmaceutical supply chain management and insurance claim processing.

Source: Cornelius C. Agbo et al., 2019

According to a Statista Research Department study “Industry leaders in blockchain technology worldwide” (2018), financial services were seen as the leaders of the blockchain technology market, healthcare hardly following with only 11% of the executives convinced. The immature and volatile state of this technology was ranked a top-3 barrier by survey executives to adopting blockchain technology in healthcare.

Nevertheless, experts predict the blockchain market to grow from half a billion USD in 2018 to 2.3 billion USD in 2021, with a market expansion in size expected to over 23.3 billion U.S. dollars by 2023[17]. In that sense, as per Till et al. (2017), blockchain could even “create new funding and capital streams, potentially bring new funders into global health”.

Besides Cornelius C. Agbo et al. (2019), whose results showed that *“ blockchain has many healthcare use cases including the management of electronic medical records, drugs and pharmaceutical supply chain management, biomedical research and education, remote patient monitoring, health data analytics, among others.”* , other articles like the one from Agbo et al. (2019) state the benefits of blockchain in the health industry.

It is surprising that relatively little research and real-life implementations has been undertaken so far in terms of the future of those technologies’ direct impact on people and

[17] STATISTA RESEARCH DEPARTMENT, [no date]. Global market for blockchain technology 2018-2023. Statista [online]. [Viewed 14 December 2019]. Available from: https://www.statista.com/statistics/647231/worldwide-blockchain-technology-market-size/

their way to manage and control their private data. It represents a massive opportunity to seize for healthcare as well as an urgent need to catch up, adapt and develop the industry.

Unfortunately, it's not yet possible to get perspective on the situation and concrete real-life implementations of blockchain use in eHealth services are lacking for now which leads to navigating in many assumptions.

2.2.3 Patient perspective

2.2.3.1 *eHealth*

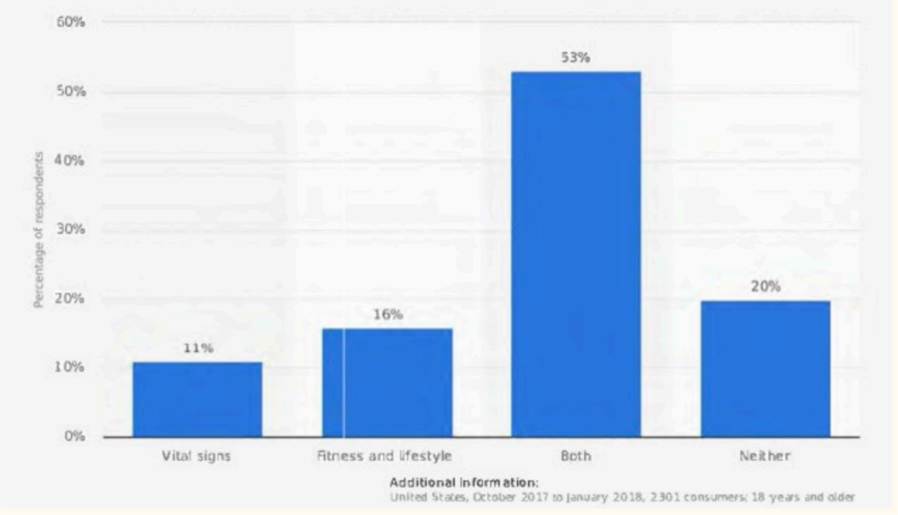
According to a European study by SopraSteria Consult (2019), on nearly 1,200 individuals from 6 European Union countries, a large majority (8/10) consider that the development of digital applications for health monitoring would improve the care provided and the quality of their country's health system. Indeed, the digitisation of patient information would make it possible not to talk anymore about independent healthcare actions but more about a healthcare pathway. As the monitoring of the path is global and continuous, the treatment generated will appear more precise and appropriate to the patient's condition. Nevertheless, some of the most advanced countries (Belgium & Norway) are already making digital tools available. Some of their residents already declare that they share personal data with medical authorities via these digital tools. The respondents stated that the expectations of these digital tools are very high with regards to the monitoring of chronic diseases, the quality of diagnoses and the speed of care management (SopraSteria Consult, 2019).

In that sense, “the presence of a chronic health condition predicates an impact on acceptance of this technology” is stated by Salgado et al. (2020) in their recent study on the drivers of mHealth acceptance and use from the patient perspective.

However, storage, confidentiality and anonymity are prerequisites that Europeans are not willing to ignore. Indeed, according to a large majority of respondents (79%), only health actors and public health authorities and institutions would be able to collect personal health data in complete confidence (SopraSteria Consult, 2019).

Indeed, even if the phenomenon of the "expert patient" tends to encourage patients to become "full-fledged actors" in their own health care (and therefore to enter and share health information of their own free will), the majority of respondents consider that the digitisation of their medical records could widen a gap of injustice (insurance, employability, anonymity, etc.) if these data are not protected. (Enquête Européenne sur la digitalisation du parcours de santé, 2019).

Figure 3 - Percentage of US adults who were willing to wear health statistics tracking technology in 2018



Source: Statista, 2018.

On the Figure 4 above it is seen that 53% of the US adults are willing to wear health statistics tracking in 2018, both for vital signs and fitness and lifestyle tracking. While 1/5 of the respondents do not want to wear health statistics tracking technology for neither of these reasons. Vital signs are the least wanted with 11% adoption will.

Results from the Statista research were similar to those of the French Ministry of Solidarity and Health, which conducted a survey on the French population in 2017[18], aiming to gather opinions on the use of connected objects in the health field. In the results, the French say they are more open to applications for well-being than for health. The major obstacles to their use oscillate between a lack of interest and a fear relating to the use of their personal data.

Considered an essential component of care, self-management is the cornerstone of good care by health professionals. In order to optimize this self-management for users, it is essential to study and understand the needs and expectations of patients in their e-health. In the study “a patient perspective on eHealth primary care”, Martine Huygens (2017) reveals the importance of self-monitoring as a prerequisite condition for their willingness to use e-health for their medical follow-up. The results of this study, conducted among people with diabetes or cardiovascular disease, led to conclusions about self-management and e-health. After analysing the results, the researchers conclude that people with diabetes tend to have a better perception of their self-monitoring needs and benefits and are the most

[18] DICOM_JOCELYNE.M, Ministère des solidarités et de la Santé, 2017.

willing to use eHealth. People with cardiovascular disease reported less need for self-monitoring support because their disease has little impact on their lives. With this research, it is understood that different diseases impact the way patients perceive the use of eHealth solutions. In addition, participants indicated that eHealth should not replace, but complement self-care.

User-centred design (UCD) is a method that must be used if patients are to be involved in the development of their eHealth. To this end, patients responded that e-Health should be easy to use and require as few actions as possible, especially for elderly people who are not familiar with the Internet or modern technologies.

Finally, the "patient perspective on eHealth primary care" study, reveals that the general opinion on the implementation of eHealth was that it should not be mandatory: the patient should be able to choose whether or not to use it. In conclusion, there are differences in the expectations and needs of different patient groups regarding eHealth for self-monitoring purposes, suggesting that eHealth and its implementation should be tailored to the patient group. The benefits that patients expect from e-Health and their perception of control over their disease seem to play an important role in patients' willingness to use e-Health for self-management (Martine Huygens, 2017).

In terms of patient's perspective on blockchain, only Gundlapalli et al. (2017), showed how patients can take control of their HER through distributed ledger technology,*" chosen specifically to meet what we see as the fundamental issue in health informatics, namely trust and security".*

2.3 Gap

Overall, it is seen that documentation on eHealth is increasing every day and is on the verge of a revolution. However, publications on eHealth are numerous but their content mostly vague due to the lack of perspective on the matter.

The need for patient data has shown to be vital, (1) for medical practitioners, (2) for the medical industry and (3) patients' outcomes. In addition, the urge to control and stop the ongoing pandemic put an emphasis on this existing need for health data.

Among all the articles reviewed for the writing of this thesis, all agree that digital health is the next lever to relieve the medical care sector and deliver better patient outcomes, by reducing mistakes19, ensuring better health facilities management20 and patient follow-up21. This evolution brings many advantages for patient care and health (better reactivity, better follow-up, health pathways instead of independent care actions).

Although the articles often deal with different themes and focus, they all mention the risks, limitations and benefits of digitisation of the medical system for the patients. However, there are privacy and security concerns about the data required to nourish and develop adequate eHealth technologies. The danger about the digitalisation of personal health data comes from biased use by organisations or theft by a third party, as well as the lack of global structured legal frameworks which would severely punish abuses.

Regarding patients, a large majority consider that the development of eHealth for monitoring would improve the care provided and the quality of their country's health system22. Patients find availability of their health data important for self-management and follow-up but express the need for free choice and privacy. Indeed, storage, confidentiality and anonymity are prerequisites that people are not willing to ignore, especially in Europe where only public health authorities and institutions would be able to collect personal health data in complete confidence (SopraSteria Consult, 2019). It has also been seen that "the presence of a chronic health condition predicates an impact on acceptance" (79%) as per Salgado et al. (2020).

19 (ENQUETE EUROPEENNE SUR LA DIGITALISATION DU PARCOURS DE SANTE, 2019)

20 (Sumant Ugalmugle, 2020)

21 (ENQUETE EUROPEENNE SUR LA DIGITALISATION DU PARCOURS DE SANTE, 2019)

22 (SopraSteria Consulting, 2019)

Regarding the legislation, cryptocurrencies and digital assets are subject to fragmented laws. Europe has an emergent good privacy legislation structure that serves as a model for the development of such regulations worldwide.

Besides, documents published by the eHealth Stakeholder group are associating eHealth with health inequalities. Marschang (2014) mentioned the socio-economic disparities and differences in treatment that can result from entering such information in digital format, including differences in profession, access to technology and knowledge. Confirmed by Latulippe et al. in 2017 on Pubmed, “eHealth has the potential to widen the gulf between those at risk of SHI and the rest of the population”.

Researches on patient’s perspective and adoption of eHealth has been conducted for years by several studies including studies of Safi et al. (2019) and Hesse and Schneider (2007). Plus, blockchain uses in healthcare are broadly studied at the moment but no real-life implementations have been registered yet. It is clear that only a few of the reviewed take into consideration the direct opinion of the patient and prefer to rely on expert statements.

Blockchain advent in the field is considered to be game-changing for its properties of innovative technology for securing and processing health data. Covered in studies for governments usage23 to pioneering implementations in digital governments, to financial, manufacturing, and retail, the possibilities are many.

However, patients’ reflections on the use of blockchain in these eHealth solutions has not been empirically searched yet. The question arising from this project is therefore relevant in the sense that it focuses on the patient’s perspective on the implementation of blockchain in these new digital health technologies. Thus, it aims to contribute at its scale to the construction of a strong foundation of knowledge for a development of a health system in accordance with its key stakeholders’ needs.

2.4 Objectives

Now that health care has been contextualized; digital health and the growing demand for data have been clearly understood, including the main challenges they pose; now that the concepts of privacy, DLT and blockchain have been clarified; and now that an overview of what has already been written on the subject has been given, the purpose of this paper is now:

23 (Ølnes et al. 2017)

- To analyse the relevance of the use of DLT systems, especially blockchain, in digital health
    - Show if the use and implementation of distributed ledger technology in digital health can allow patients to evolve in a digital health world which respect their needs and rights, especially privacy right.
    - Present Bowhead Health: gather, measure and analyse Bowhead Health users' insights and study the uniqueness of this concept. Indeed, they are the first ones to use blockchain to secure patient data for now (possibilities, what are the constraints, requirements and benefits, patients' outcomes)
- To analyse if blockchain could play a role in a faster adoption of digital health technologies by patients
- To understand how it may generate better patient outcomes
- To generate food for thoughts and recommendations for further research

This research is not trying to find solutions to the transition towards digital health but only analysing the relevance, role and usefulness of blockchain in the process and its impact on patients. If the study shows that potential factors or additions to the blockchain are needed to facilitate this transition, they may be suggested in the Conclusion for future research. The governance framework is not studied in depth and shall require further research. Also, a full study of blockchain technology performance and overview of its providers in the healthcare industry is beyond the scope of this publication.

3. Methodology

The role of this Methodology section is to provide empirical data for determining if distributed ledger technology systems can accelerate the adoption of eHealth by patients. The goal of the following empirical work is to add material to the literature by delivering answers to the latter question with recommendations backed-up by data.

3.1 Study design

The study was designed and conducted as an exploratory research, aiming to gather empirical qualitative and quantitative data through surveys and interviews, as well as a description of a real implementation case. Quantitative data search, involving primary and secondary data on those different sources permitted to measure user satisfaction, retention rate, needs and feelings towards the concept, perspectives, daily use and other significant behavioural data.

To begin this research, secondary data were gathered to create an in-depth understanding of the context as well as to set a foundation of knowledge for further research. These data entirely came from external sources such as national health organizations, National institutes of Health (NIH), WHO, governments and academic papers found on Google Scholar, University of Cambridge, the US National Library of Medicine National Institutes of Health (NCBI). Once these former data were processed, interviews with professionals and patients were conducted with respect to GDPR.

3.1.1 Collaboration with Bowhead Health

Bowhead Health, founded in December 2015, core value proposition is privacy and protection of the identity of the users. They believe that blockchain, especially distributed ledger technology, can enforce health data privacy and secure ownership for already 75'000 users and their health data. The start-up works with Anonymized Healthcare Token (AHT) which uses smart contracts to produce enforceable flows. Hence, Bowhead provides to researchers the possibility to receive totally anonymized health data and thus participate in research advances, especially in the area of mental health.

Besides, the company, aiming to reach better health outcomes, has developed innovative prototypes of devices and technological tools to facilitate patient's life and deliver better care. First Place at Boston Biotech Start-up Week in 2019, they received a big investment from a pharmaceutical packaging manufacturer in the past, signed a major diagnostic company, partner with DNA Lab and continue to grow many other partnerships with strategic healthcare industry actors to foster a safe way towards the digitization of the health care system. Bowhead Health agreed to collaborate for the secondary data research phase of this report to show that real-life implementations of DLT systems in healthcare are possible, efficient and bring huge value.

3.2 Recruitment and sample

3.2.1 Quantitative data

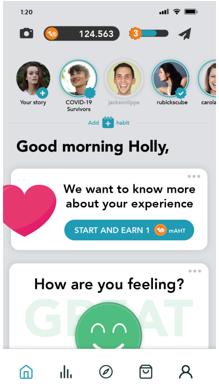
First, the goal was to get access to a broad sample of people and patients. A global anonymous survey in two languages, French and English, was created to allow a lot more people to have access to it and fill it. The participants were recruited online, through personal and professional networks. It aimed to represent a population as a whole by reaching a broad diverse sample from various countries and socio-economical characteristics, different professional life, religion, education and background. In addition to the valuable data it conveyed, it also served to test the efficiency and relevance of the questions to develop for an additional future survey.

Sample 1: A 14-questions online survey counting 68 answers (see Appendix 1).

- 2 versions: French and English.
- The surveys have been online for two months from June 1st to August 14th, 2020. It was shared on LinkedIn, and on personal networks.
- Broad diverse sample aiming to represent the population as a whole.
- Data were gathered on use of digital health technologies; satisfaction; perceptions of eHealth; motivations and potential benefits to share data; knowledge and trust in blockchain technology; future of healthcare.

Then, to get a more focused sample, a survey was implemented in the Bowhead Health application, recruiting the daily users of the tool. This sample was relevant to the study since it aimed to gather targeted data: current users of digital health technologies, more specifically mobile Health (mHealth). Mobile health being one of the rising stars of the digital health industry, this in-app survey represented a key opportunity to gather their direct input, thus limiting the intermediaries and trusting the source of the data. Indeed, getting their vision, thoughts and feelings on the use of DLT systems to protect privacy is strategic for the analysis of the drivers and motivations to adopt health technologies.

Sample 2: A 4-questions in-App survey targeting eHealth users and specific patients counting 747 participants (see visual in Appendix 2) was conducted. This survey was the fruit of a close collaboration started in December 2019, with the mobile application and company Bowhead Health Inc., based in Toronto, Canada.


Good morning Holly,

We want to know more about your experience

How are you feeling?

- It was implemented on the homepage of the app and users were incentivized with 1 Bowhead mAHT to answer the questions and thus increase the number of participants.
- Data were collected from 15th June to 14th August 2020. Two data reports were sent by Bowhead Health to track the incoming flow of data.
- Information were gathered on: reasons for adoption; knowledge and trust in blockchain technology; perception of health data safety. Then, a breakdown to their locations and potential diseases could also be tracked.
- Later, in addition to the data already collected on the users, we were able to analyse the ones who are currently suffering from a chronic illness or severe disease. The latter allowed the research to get more primary data and insights on the group of interest, patients.

3.2.2 Qualitative data

Qualitative data for this report came from interviews with professionals and patients. It is during this phase that key qualitative learnings could be outlined and that understanding of most of the theoretical concepts was possible.

First, gathering the vision of professionals and leaders in the field of eHealth, blockchain technologies, and private innovative start-ups added a considerable value and perspective to the direction of this project. The professionals were recruited thanks to the Internet and later, based on the several discussions' insights from Mr. Diaz-Mitoma Jr. interviews and the experts themselves.

4 qualitative interviews with professionals in eHealth and blockchain (see transcriptions excerpts in Appendix 3):

- Francisco Diaz-Mitoma Jr., CEO and co-founder of Bowhead Health Inc.
- Pierre-Mikael Legris, CEO and co-founder of Pryv
- Alexis Roussel, COO of Nym

- Anonymous Data Analytics Manager in the Healthcare industry

Furthermore, people who currently suffer or suffered from a specific disease (chronic illness or severe disease) were interviewed, aiming to understand patients' perceptions, thoughts and relationships towards digital health technologies. They were recruited after a "call-to-interview" publication on professional networks and communications with several patient associations, the latter were often very sensitive and did not want to add additional anxiety to their patients' lives with interviews. For this reason, this sample is not very large.

3 qualitative interviews with current and cured patients (see interviews excerpts in Appendix 4) found through local network and patient associations. Again, for anonymization purposes, the first names of the interviewed patients were replaced by aliases.

- Marc, engineer, suffers from a "Pneumopathie chronique à éosinophiles"
- Sophie, member of a patient association, suffered from breast cancer
- Anna, retired and member of a patient association, suffered from colon cancer

Please note that, since the samples are not of a high number, it implies that further statistical research can study the subject on bigger samples and compare the findings with the current report.

3.3 Data collection and analysis

The secondary and primary data were collected between January 2020 and 14th August 2020. Information were extracted as raw data from the surveys. Questionnaires' answers were sorted with Tableau Prep, processed and analysed through Tableau Desktop and Microsoft Excel to create tables and particular figures.

General online surveys' respondents were communicated the academic purpose and context of this study, the following mention to GDPR was included in the online survey description: *"With respect to GDPR (2016), no identifying data will be collected except for your gender and age range. The data will be processed on Tableau Desktop and Microsoft Excel, to be able to confirm or refute my hypothesis."*

Regarding the in-app survey, data were collected in collaboration with Bowhead Health who provided two raw data reports from their mobile application and counselled on the elaboration of some of the related figures. Two time periods were covered, the first one extended from June 15th to July 30th and the second from July 31st to August 14th. As the data collected during the second period of time did not show any significant differences in terms of assumptions, they were considered as one unique sample of users. Besides, the fact that only a few questions (4) could be implemented in the app limits the possible comparisons with other samples but provides material to reflect.

For the interviews, a systematic presentation of the context, purpose and public character of the research was done prior to the discussions. Professionals and patients' consent were asked to record the interview as well as to publish their identity in the final report. Hence, to preserve patients' right to privacy, their first names were intentionally replaced by aliases. Though, the value of their contribution is nonetheless diminished.

To process the interview findings, a manual analysis was performed. Systematic themes were created by focusing on redundant keywords, sentences and suggestions highlighted in the interviews and surveys. After gathering the important keywords, they were first placed under a corresponding category: digital health technologies, distributed ledger technology/blockchain, healthcare system. Next, they were grouped together in sub-themes based on their subject and relevance: No evolution/Slow evolution; Digital integration; Telehealth focus; Covid-19 as a driver; Potential benefits/ Innovation; Importance of Security/transparency; Concerns/Risks and misuses.

4. Analysis

This section provides the analysis and comments to the collected data.

4.1 In-App survey

Consisting of 4 questions in the mobile application Bowhead Health (see Appendix 2), the sample size is 747 participants.

Figure 4 - In-app survey answers, by continent

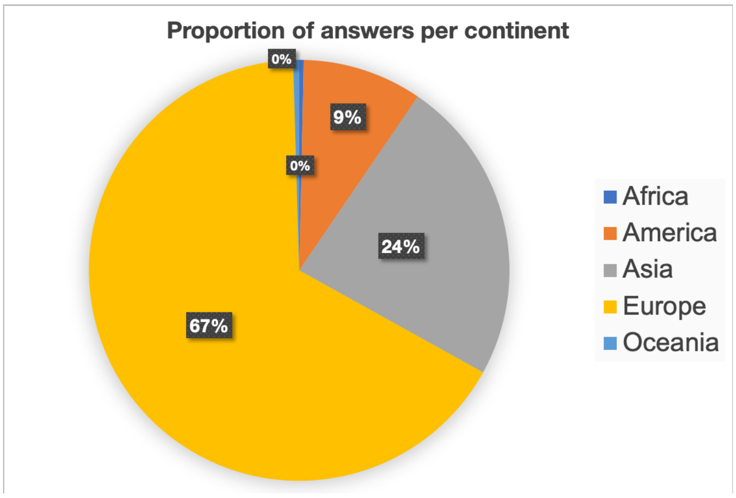
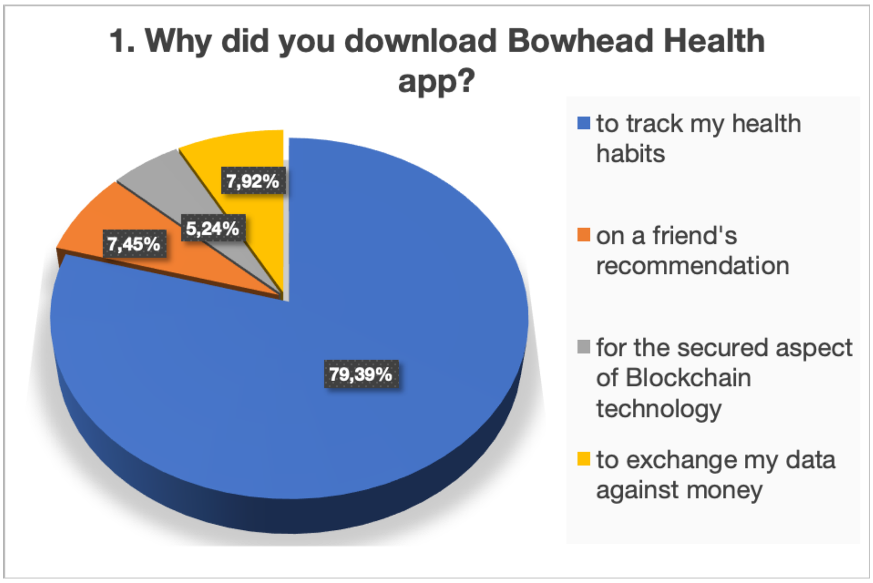


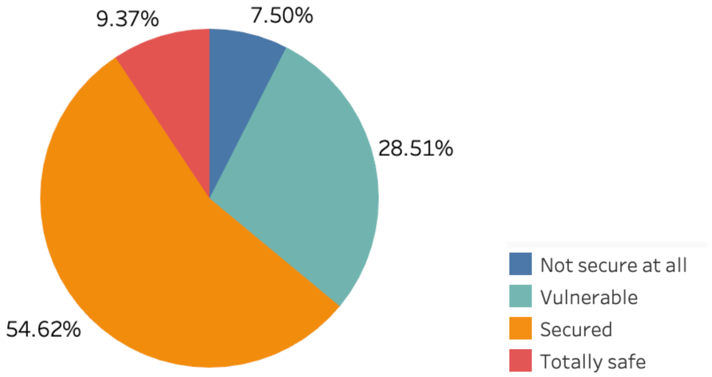
Figure 4 shows the in-app survey's total answers geographical breakdown. Most of the answers received came from Europe and Asia with respectively around 67% and 24% total records. America represents 9% of the sample. Oceania and Africa being the two less represented countries, with respectively around 0.47% and 0.35% presence.

Figure 5 - Reasons for mobile application adoption



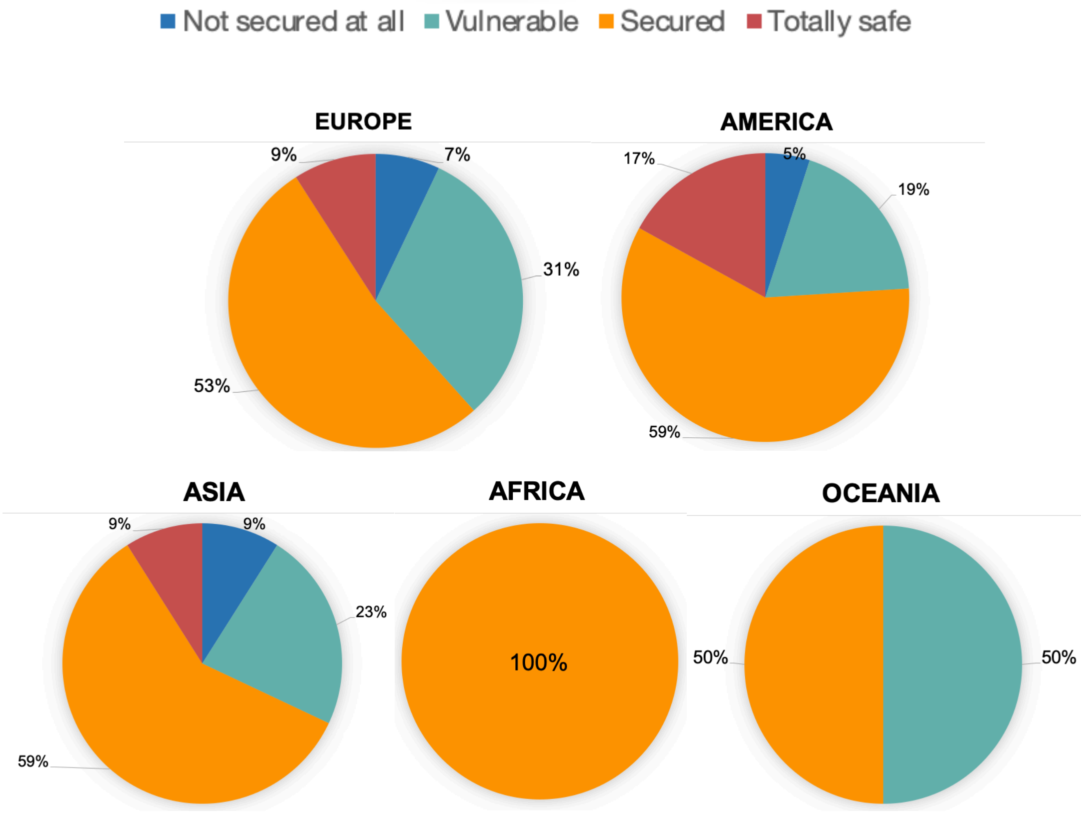
The pie chart above clearly pictures why the majority of the users downloaded the application: to track their health habits, 79,39%. Followed by far by persons who purchased it *to exchange data against money* (7,92%) and *on a friend's recommendation* (7.45%). *The secured aspect of blockchain technology*, was the least chosen option, users tend to not to place it at the core of their purchase decision of the mobile application.

Figure 6 - Users' perception of their health data safety



As pictured by Figure 6 above, to the question *"In general, how safe do you believe your health data are?"* people tend to think their health data are *Secured* at 54.62%. Followed by 28.51% who believe they are *Vulnerable*. The smallest part of the users, 7.5% declared feeling their data are *Not secure at all,* while 9.37% think they are *Totally safe.*

Figure 7 - Users' perception of their health data safety, per continent



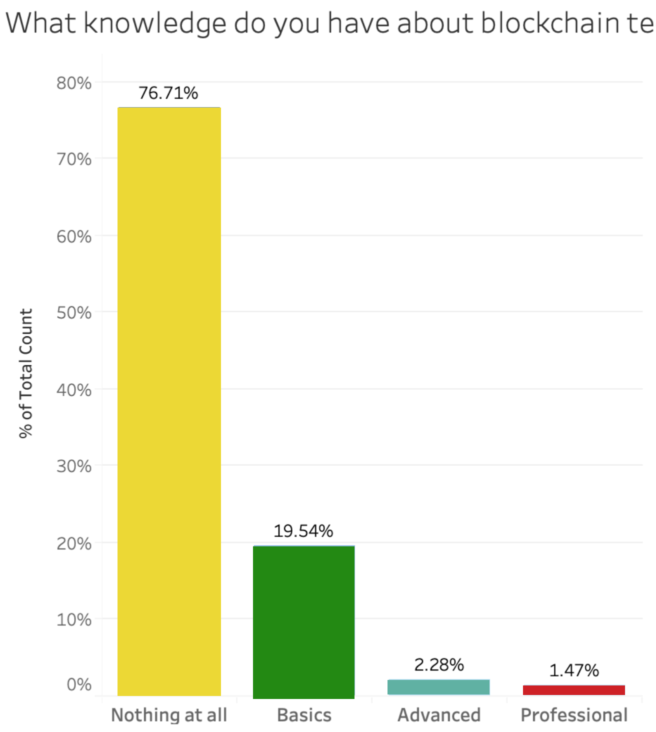
[24]

As per the results displayed on Figure 7, the research showed every continent's perceptions of its data safety. As a result, in every continent, more than half of the users trust their health data are Secured. Out of 571 answers from Europe, 52% of these concluded their health data were Secured. 31% of Europeans believe their health data are Vulnerable while 7% believe they are Not secure at all.

America is the continent in which people have the most confidence in their health data, people declared their health data were *Totally safe* at 17% (against 9% in Asia and Europe) and *Secured* at 59%. 100% of the respondents (3) from Africa trust the security of their health data. In Asia and Europe, the confidence is less present. 9% of Asians believe their information are *Not secured at all*, while 23% mentioned *Vulnerable*.

[24] Based on question 1 total answers, 859.

Figure 8 - Users' knowledge of Blockchain technology



	% of Total Count	Number of answers
Nothing at all	76.71%	573
Basics	19.54%	146
Advanced	2.28%	17
Professional	1.47%	11
Grand Total	**100.00%**	**747**

Then, on Figure 8 it is exposed that a great number of participants, 76.71% (573), do not have any knowledge of blockchain or DLT whatsoever. When grouped with *Basics* knowledge, it results that 96.25% (719) of the participants do not have *any knowledge at all* or only *basics*. The survey attracted 17 people who have *Advanced knowledge of blockchain and* 11 *Professional* skilled people in total.

Figure 9 - Users' trust in Blockchain technology in securing health data

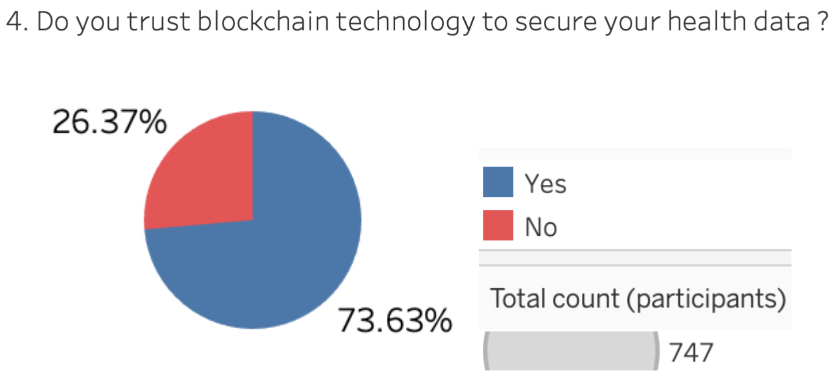
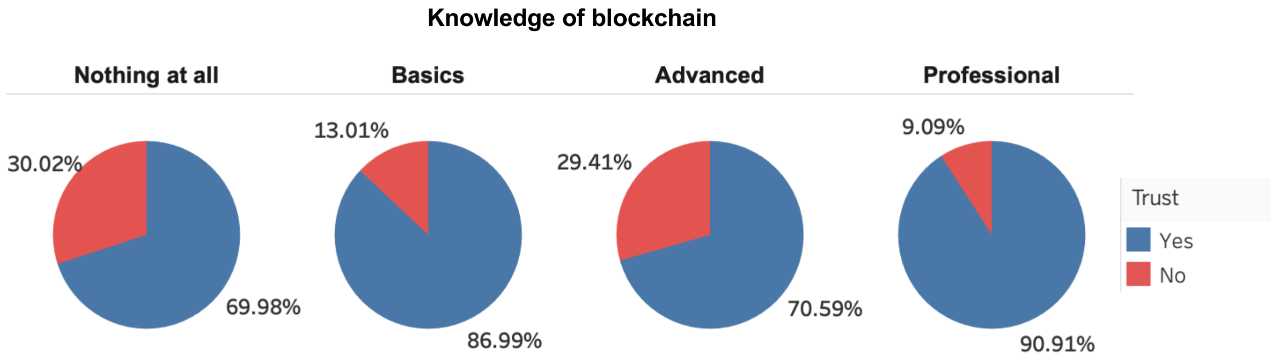


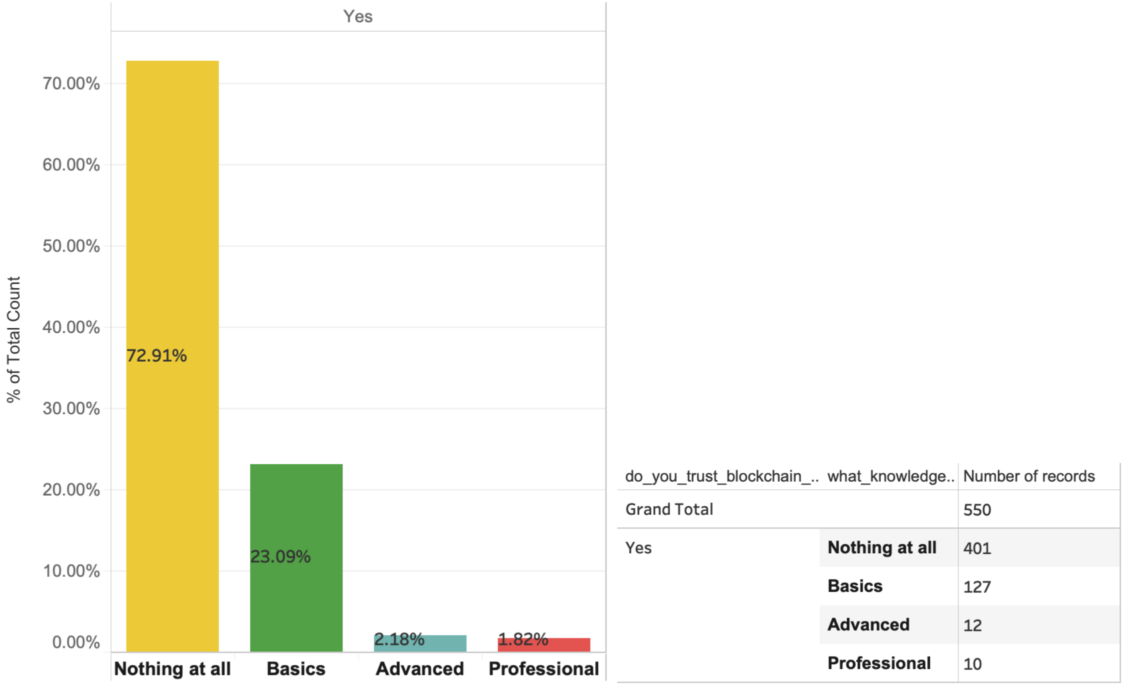
Figure 9 outlines that the overall trust level in blockchain for 747 participants is 73.63%, representing 550 users, as of around 26.37% (197 users) do not trust it.

Figure 10 - Relationship between knowledge and trust of blockchain technology to secure health data



However, cross-figures of the relationship between knowledge of blockchain and trust in the technology show that even though some of respondents do not have any knowledge of blockchain at all, 69.98% of them trust it. The ones who have only basic knowledge trust it at 86.99%. Professional skilled people in the field trust this solution to secure health data at 90.91%, while advanced skilled persons confidence level is of 70.59%.

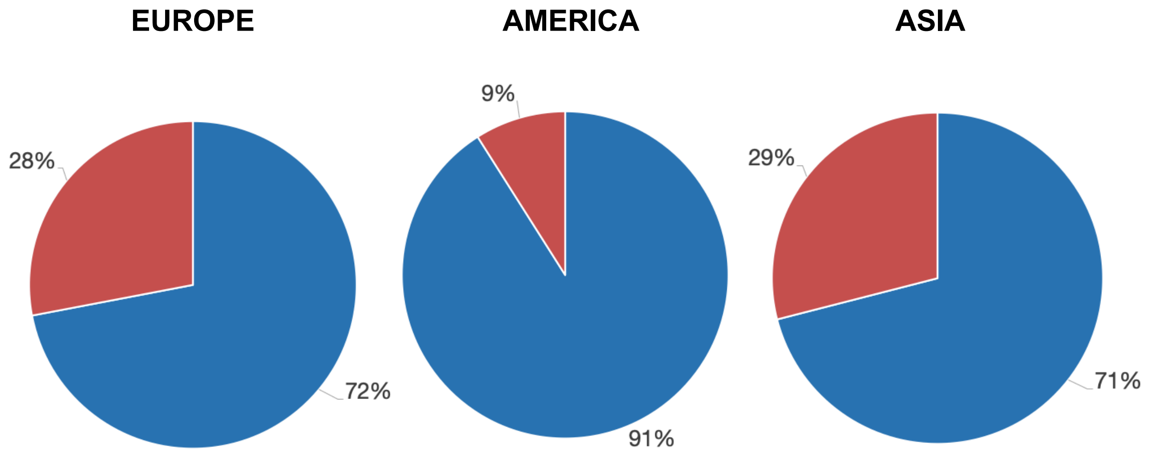
Figure 11 - Relationship between people who declare trusting blockchain and their knowledge of the subject



do_you_trust_blockchain_..	what_knowledge..	Number of records
Grand Total		550
Yes	**Nothing at all**	401
	Basics	127
	Advanced	12
	Professional	10

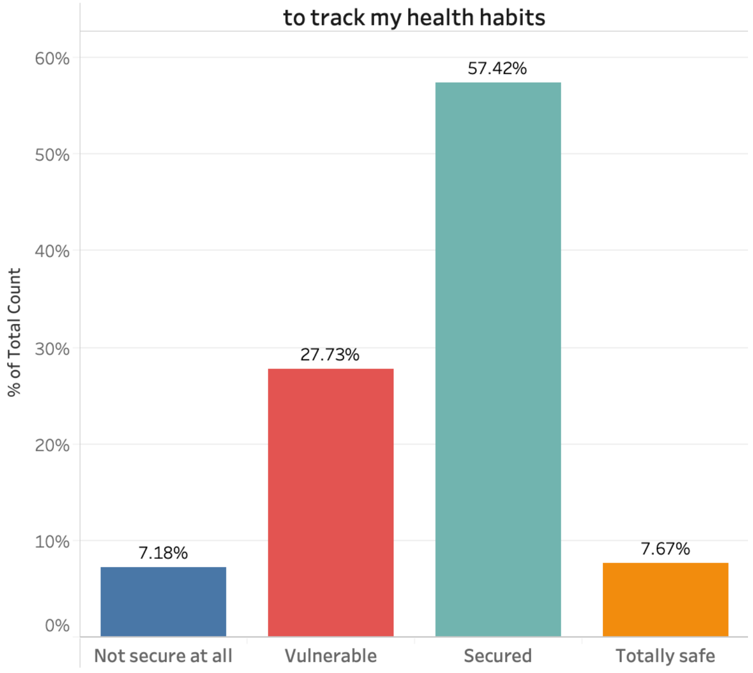
As stated in Figure 11, 550 people answered *yes* to the question: *Do you trust blockchain to secure your health data?* From these people, it shows that 96.25% (528) do not have *any knowledge of it at all* or only *basics*. Besides, 4% (22) of the people who trust blockchain are *Advanced* or *Professional* in the subject.

Figure 12 - Trust in blockchain technology to secure health data, per continent



The pies of the Figure 12 present the overall trust in blockchain that Europe, America and Asia have. Africa and Oceania being 100% confident in blockchain. Americans are the most convinced with 91% trust in the technology. Europeans follow with 72% trust. Asia is the most sceptical continent with 29% of the respondents not trusting blockchain to secure their health data.

Figure 13 - Primary reason for adoption versus users' perceptions of their health data safety



The Figure above compares answers from Question 1 and Question 4 of the in-app survey: 1. *Why did you downloaded Bowhead?* and 2. *How safe do you believe your health data are?* Considering the people who downloaded the mobile application *to track* *their health habits* (Question 1), more than 57.42% think their data is *Secured*, around 27.7% of them believe it is *Vulnerable* (Question 2). Only a small proportion of them believe it is *Totally safe (7.67%)* or *Not secure at all* (7.18%).

Table 7 - Proportion of participants suffering from a particular disease

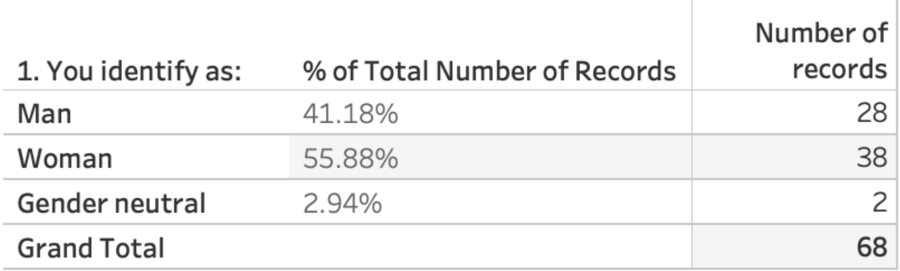
Disease	**Total # answers**	**% of Total records**
Anemia	3	1.54
Acute Depression	1	0.51
Acute Gastroenteritis	1	0.51
Acute Herpes Zoster and pain	2	1.03
Acute Myeloid Leucemia	1	0.51
Adenomyosis, Endometriosis	1	0.51
Adult Atopic Dermatitis	1	0.51
Allergy	1	0.51
Anorexia Nervosa	1	0.51
Artrosis of the Knee	1	0.51
Asthma	35	17.95
Atypical Trigeminal Neuralgia	1	0.51
Auto-immune Thyroiditis	1	0.51
Bacterial Pneumonia	1	0.51
Chronic Plaque Psoriasis	1	0.51
COPD	4	2.05
Diabetes	17	8.72
Epilepsia	2	1.03
Facial Neuralgia	1	0.51
Heart disease	9	4.62
Hypertension	26	13.33
Lupus	1	0.51
Menstrual related abnormalities or distress	5	2.56
Obesity	76	38.97
Sciatica or Sciatica Pain	2	1.03
Total	195	100

The table 7 shows the 195 persons (26.1%) out of 747 total respondents, who suffer from a particular disease. It can be highlighted that more than ¼ of the sampled people are in fact real patients, while the rest have no specific health disorders to declare. Asthma (17.95%), Diabetes (8.72%), Heart disease (4.62%), Hypertension (13.33%) and Obesity (38.97%) being the most represented health issues. These people are a non-negligent part of the users.

4.2 Online survey

Consisting of 14 questions in an online survey, the sample size is 68 participants (see Appendix 1).

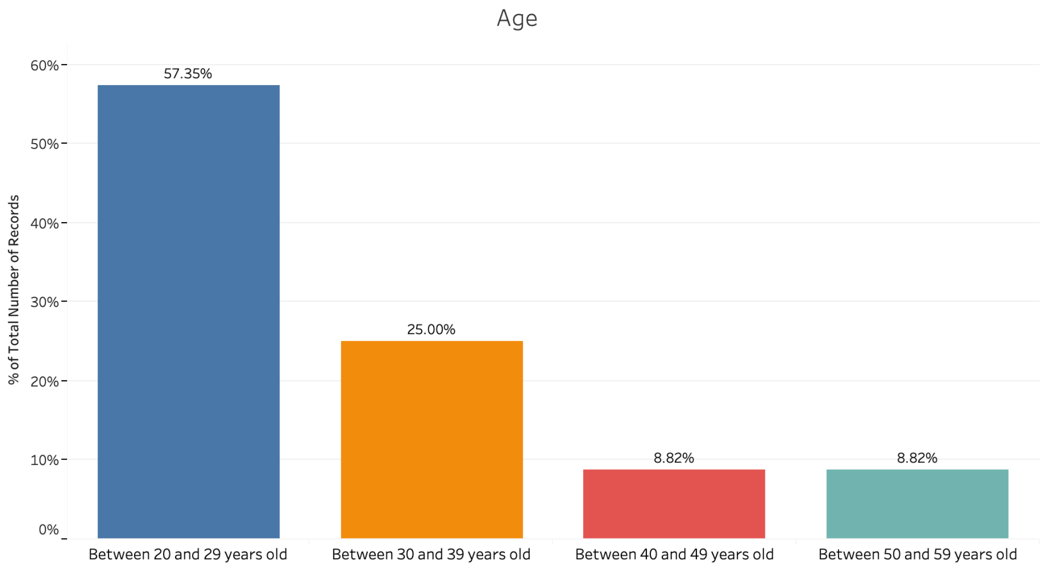
Table 8 - Online survey sample gender



1. You identify as:	% of Total Number of Records	Number of records
Man	41.18%	28
Woman	55.88%	38
Gender neutral	2.94%	2
Grand Total		68

Regarding the gender segmentation of the sample 1, including 68 people, around 55.8% (38) are women, around 41% are men and 2,9% (2) are gender-neutral, which make this sample diversified and almost equally representative.

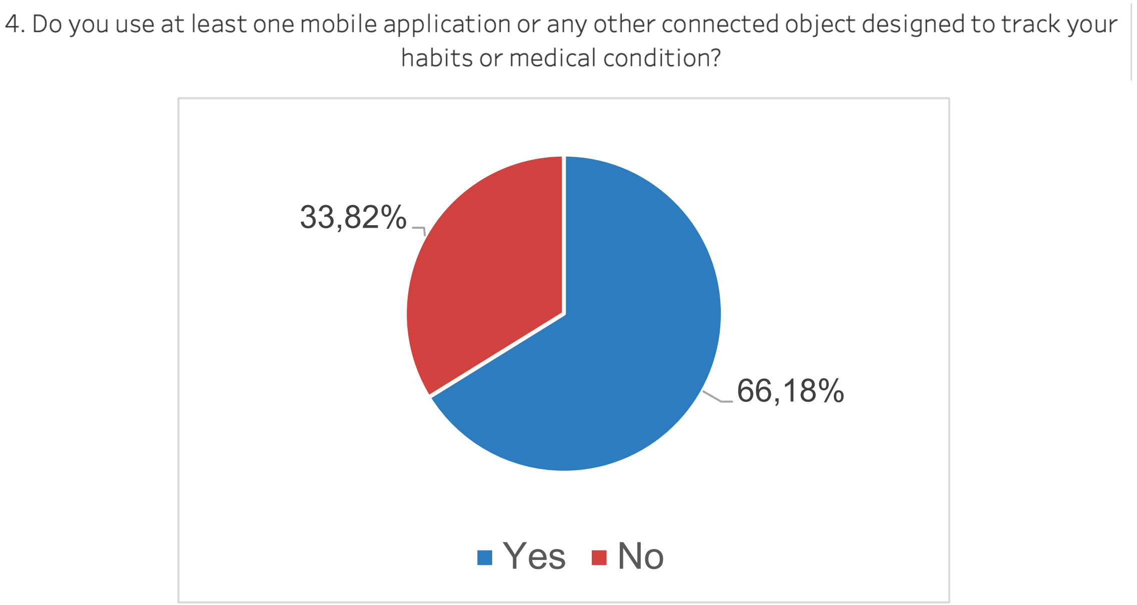
Figure 14 - Online survey sample age segmentation



When looking at age segmentation, the majority of the respondents are *between 20 and 29 years old,* representing the young generation, more at ease with eHealth technologies in theory. It also shows that there is an under representation of people over 40 years old, 17.6%. However, this does not impact the data that gathered and its related findings, since it still has a representation that shows the mindset of the 20 to 29 years old group, which will be the next generation of digital health technologies users through ICT. Besides, the 30 to 39 years old are represented at 25%, which is still a good ratio.

Overall, the validity of the data remains since the major part of the population covered is the people that tend to use eHealth technologies more.

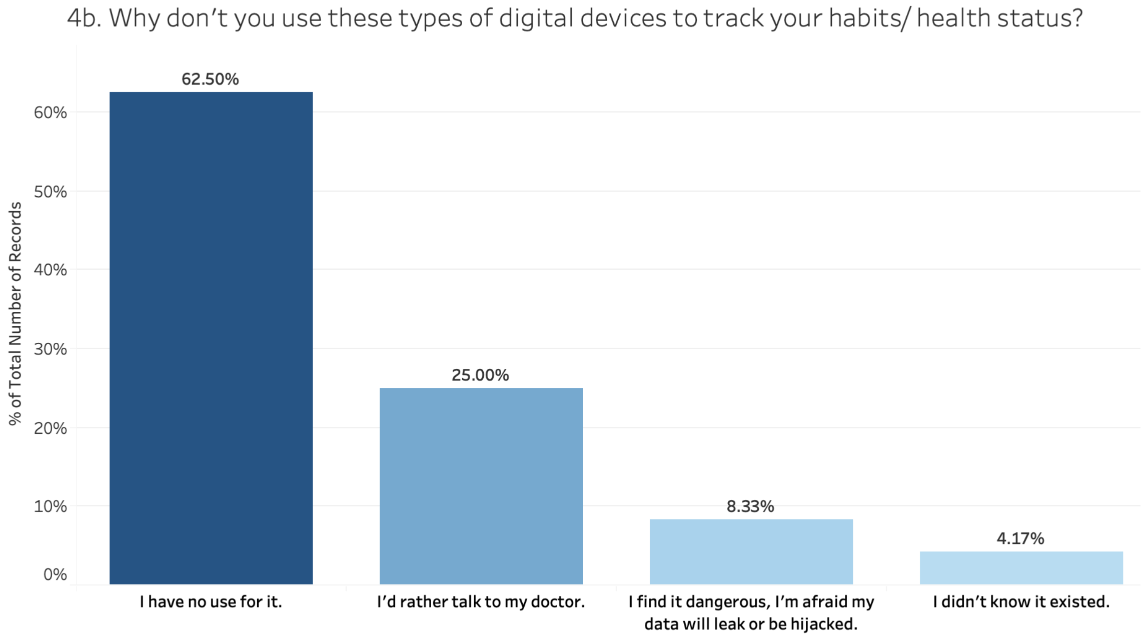
Figure 15 - Use of connected objects for tracking health condition



66.18% (45) of the participants declared using at least one mobile application or any other connected object designed to track habits or medical condition.

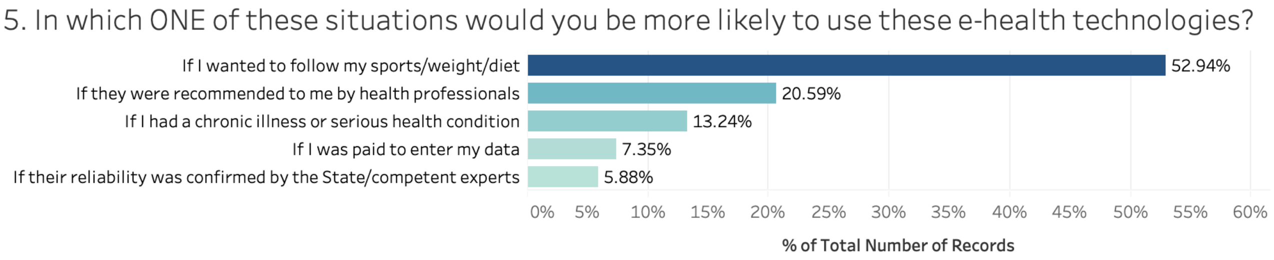
Another question detailed the type of devices these 45 participants cherished the most: 39,7% use a mobile application on their smartphone, 25% use a watch or other connected device, 1.47% use something else. But still 33.82% (23 persons) do no use digital health technologies (devices) and below are some of the reasons why.

Figure 16 - Reasons not to adopt eHealth technologies



As shown in the Figure 16, the majority (62.5%) of the participants affirmed not having any use for such digital devices, while ¼ would rather talk directly to their doctor. Finally, 2 (8.33%) find it dangerous and 1 did not know these existed. However, with the following graph, an attempt was made to understand in which situation these people could eventually start to use these technologies.

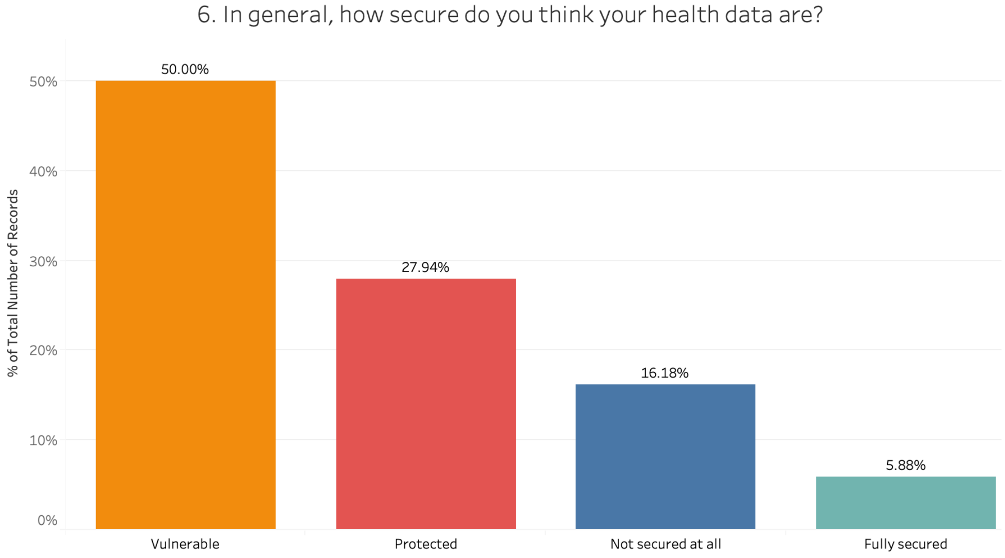
Figure 17 - Situation in which users will tend to adopt a eHealth solution



As a result, 52.94% (36 persons), would use digital health technologies first if they wanted to *follow their sport evolution or diet*. Then, if a health professional, such as a doctor or a pharmacist, would legitimately recommend it to them (20.59%). The last top-3 situation in which they would use it is, if they faced *a chronic illness or a serious health condition* (13.24%).

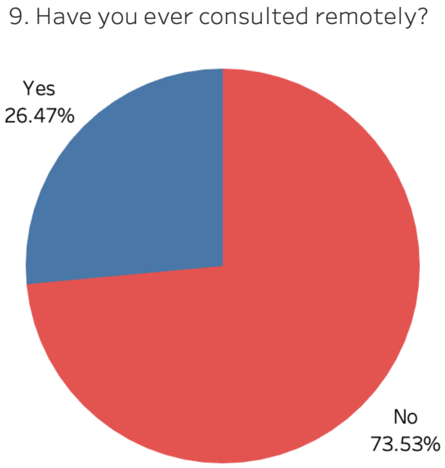
Receiving a compensation to enter their data only convinced 7.35% of the participants. Lastly, a confirmation of reliability from the State or competent experts, 5.88%, does not seem to influence the adoption of these technologies by the survey's respondents.

Figure 18 - Participants' opinions on the safety of their health data



50% of the people surveyed online believe their health data are *Vulnerable*. 27.94% of them think they are secured, while 5.88% trust they are *Totally safe*. Still, 16.18% of the respondents think their health data are in general, *Not secured at all*.

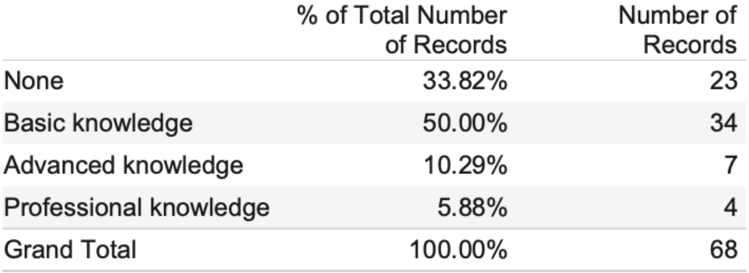
Figure 19 - Proportion of people who have ever consulted remotely



Then, the results of Figure 19 show the proportion of people who have ever consulted remotely, especially valuable as the survey was conducted during the 2020 quarantine. Consequently, nearly ¾ (73.53%) of the participants declared having never consulted remotely.

From the 26.47% (18) people who have consulted remotely in the past, another statistic's results from this survey show that 50% of them were *Partially satisfied* of their remote medical session, 40% were *Satisfied* and 10% only were *Very satisfied*.

Table 9 - Knowledge of blockchain technology, online survey

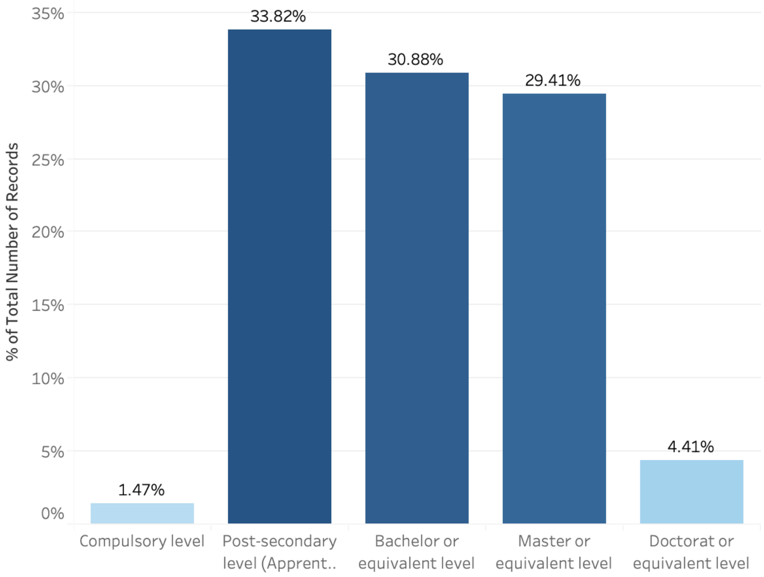


	% of Total Number of Records	Number of Records
None	33.82%	23
Basic knowledge	50.00%	34
Advanced knowledge	10.29%	7
Professional knowledge	5.88%	4
Grand Total	100.00%	68

Table 9 displays the respondents' knowledge of blockchain technology. In this sample, the majority of the people declared having Basics (50%), or no knowledge at all of blockchain technology (33.82%). While it has been seen that in sample 2 (users of the app), the majority (76.71%) knew *nothing at all* about blockchain, as per displayed by Figure 9.

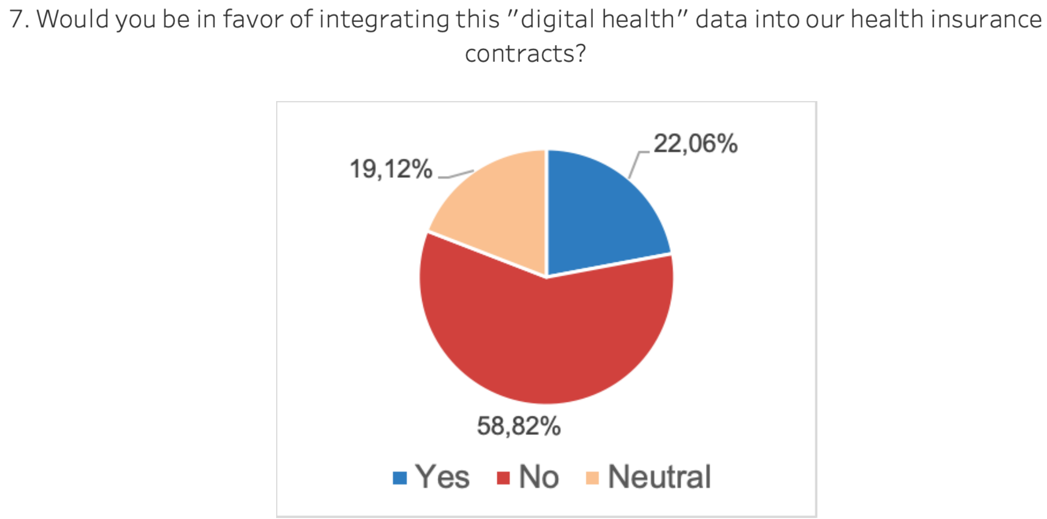
This slight difference can potentially be explained by the fact that the online survey pictured by Table 9 above, was also shared on professional networks, while sample 2 survey was only shared on the mobile application. This may have impacted the results and thus shifted the knowledge from *none* to *basic knowledge* in this sample 1, in which people with higher education are evenly represented, as shown by Figure 21 below.

Figure 20 - Level of education



In this chart we can see how the population covered by the survey was focused on educated people. This is the result of posting them on professional networks. This helps to conclude that even if people are educated and represented nearly equally in the sample, up to Master or equivalent level, they tend not to have strong knowledge of blockchain (see table 9). A hypothesis would be that the 4.41% of *Doctorat or equivalent level* are the ones who answered *“Professional knowledge*” in Table 9 previously.

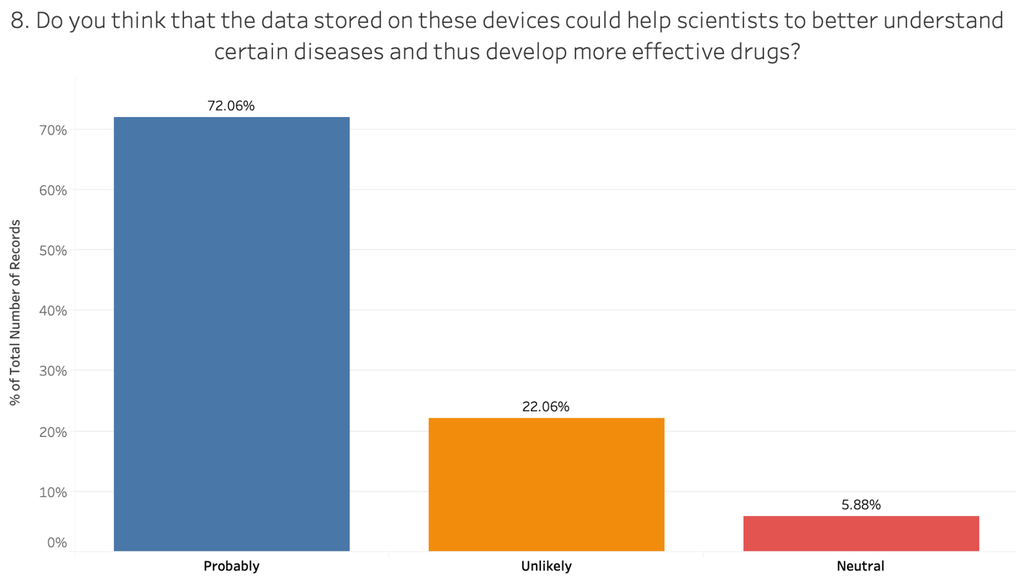
Figure 21 - Integration issue of health data into health insurance contracts



7. Would you be in favor of integrating this "digital health" data into our health insurance contracts?

On Figure 21 it is shown that a majority of the participants are against the integration of their health data into health insurances contracts, while 22.06% are in favour.

Figure 22 - Opinions on data contribution to science



8. Do you think that the data stored on these devices could help scientists to better understand certain diseases and thus develop more effective drugs?

The majority of the participants think the data stored on eHealth solutions could probably help scientists develop more effective drugs, while 22% believe it is unlikely to help. This could be studied in further research.

4.3 Summary of the interviews

4.3.1.1 *Experts*

In the experts interviewed, the common themes were the following:

Need for legal framework and Guidelines on data collection

In times of COVID-19, Mr. Diaz-Mitoma Jr. raises the following unanswered questions and alerted on the privacy risks of the process of collecting health data, especially in the urgency of a sanitary crisis. *« What happens to all of that data? Who's owning that data, who's managing that data? Who's accountable for that data?. This would be good on a policy perspective of kind of having some guidelines."* He also mentions that the "enforcement of health data standards is driven by the government in Europe". Thus, people may think they are safer in Europe compared to US where Apple, Google and other companies stand.

Privacy concerns and Blockchain

« If you want to industrialize such product, you have to be extremely concerned by the privacy of persons ». said Mr. Legris in the interview. Privacy was a common theme between the four experts. All agreed that health data cannot be stored on a blockchain. Because it would mean that the data are spread around multiple tenants who would have time to crack it down. Plus, there is no way no way that you can erase data from the blockchain. Thus, it does not comply with GDPR since it does not provide the right to be forgotten, the right to ask for the deletion of all of someone's health data in the system. *« Some people will tell you just have to throw away the keys. But you know that the data is there »* P.-M. Legris.

All experts also agree to say that blockchain is only an enabler and can help with privacy, but there are in fact several components that make up data privacy, such as using the right kinds of encryption, "*there's many different components that need to be considered such as the internet service provider, server, wifi, etc.",* as per the CEO of Bowhead, Francisco Diaz-Mitoma Jr.. Another expert in analytics in health care added *"it should help basically getting quality. And once you get data of quality and then you get data into quantity, so basically you get quantity and quality.*

Blockchain, Smart contracts and Informed Consent

Smart contracts appear to be the only realistic use of DLT for processing health data for the experts who all rely on its very design. "*Informed consent is king*" said Mr. Legris. Particularly, for use in clinical trials. If the data has been modified, with blockchain and smart contracts "*you can prove that the database has been modified, and that the clinical trial is invalid."*

Educate people on blockchain

There is lot of room for improvement in that direction as per Mr. Diaz-Mitoma Jr.*, "we should explain blockchain or we explain our how security works, so that people are more cautious about how they use different products related to their health data."*

Also, the interview of Mr. Legris highlights the fact that trust is not necessarily linked to knowledge. The latter provides a valuable comparison between blockchain (DLT) and banks. Indeed, *"for example, we trust our bank, but we don't trust it because they're super good, we trust it because they send us a statement every month of what happened to our account".* In that sense, he adds that the eHealth companies who will send detailed transparent reports to their customers will become well-rooted trusted databases. He added, *"The general public will not think blockchain. They will trust the actors responsible for using it to ensure security."*

4.3.1.2 *Patients*

First, the interview with Marc, a French engineer who suffers from a "Pneumopathie chronique à éosinophiles", a rare chronic lung disease treated only in hospitals, brought the following points:

- In general, he outlines the lack of communication between hospitals, indeed information is not shared between doctors. *"If the patient does not dedicate himself fully and participate actively in his treatment process, it allows the practitioner to reinterpret the information and provide various different diagnostic"* due to his personal experience or the diverse sources of knowledge he might have at his disposal. The patient had to travel to several hospitals located in different regions of the country. He was then constraint to reexplain his medical path and disease over again as communication between infrastructures are limited to letters and emails, and thus subject to numerous medical errors.

- It results of waste of time and stress caused by going back and forth to the hospitals for prescriptions of antibiotics and related drugs to treat the secondary effects of these antibiotics. For that, as per Marc, eHealth could have greatly helped (e-prescriptions).

- Health infrastructures are incapable of handling such amount of health data. Privacy is important for him, but an emphasis was made on the fact that healthcare actors in his sense are totally overwhelmed by events. *"Data are completely lost. So I am not afraid of sharing my data since they are unable to process them correctly for now".*

- "*data should be centralized regionally or at hospitals level at least, so that a database can group people who have the same disease and show the different treatments prescribed".* Allowing doctors to refer to a strong foundation of health care practices on rare diseases.

- Health issues are really personal for him and he does not want to be recorded as the "sick person". Even if no personal information is gathered by eHealth, he is still afraid that "one's managed to find him".

- His chronic disease affects his will to give his health data since he "does not want to be stigmatized as the sick person". Nevertheless, he would give his data for clinical research without no hesitation if some research was conducted for his rare disease.

- However, he is open to the integration of blockchain in eHealth, he mentions that "if it goes through blockchain and is then fully anonymized, why not"

Sophie

- "I think a bit of it could have been done digitally" mentioned Sophie, an active American survivor of breast cancer, when talking about the recurring weekly or bi-weekly medical appointments she had to attend. Sometimes she would just go for *"checkup and basic questions (…) and that was it.".* As it could save stress and a trip, she would agree to have consultations online.

- Hesitant to put really personal information on an app for other purposes than information or sport, she would agree to give up on some of her personal data if it could help scientists in the development of medicines or in clinical trials. "*If using my information can help professionals or scientists develop something or come up with an idea that can help someone else in the same situation then, why not".* In addition, she believes suffering from a chronic or severe disease increases the propension to share health data.

- Her biggest security fear being the insurance companies or third parties that could use her health data to make unfair decisions, *"my only level of skepticism is insurance companies now".*

- Nevertheless, she loves digital technology but find *"it lacks the human touch and human touch in the medical field, especially in the cancer area is so important.* Highlighting the constant need for guidance and support that patients require even after the end of a treatment.*"I think there are areas where digital technology is perfectly placed and (…) there are areas where I think that personal touch is still the most important thing. So why not combine the two?"*

- Sophie fears more for her data security now than years ago.

- When presenting the idea of a dashboard to control health data accesses and consents, she replied yes, "I think the more transparent it is, the better".

- Also, she believes eHealth solutions would be more spread if recommended by HCPs, but alerts on the fact that "people who are sick are vulnerable", so the safety of these applications' should be ensured in order for the most vulnerable people not to be fooled.

Finally, for Anna, an English lady who suffered from colon cancer in the past, human touch is also essential, since she *"really felt the need to go and have a long chat with the oncologist to (…) that was very important",* outlining the importance of face-to-face chats when announcing bad news. Her experience with a doctor constantly looking at his screen while enouncing some figures marked her.

- Hence, the doctors' lack of training on these technologies use is obvious
- She had never used any digital health technologies nor DLT systems but already agreed to be the subject of a clinical study at HUG, hence she is open to give her data for medical research.
- She rises a concern regarding the health insurances access to private health data for misuse

Overall, patients' feelings toward the concept are positive but they need to be reassured on privacy, safety and the final use of their data. They see eHealth as an opportunity for the system to reach better care but recognize certain threats. Their health needs have to be taken into account and not lost in the transition process, while maintaining human contact, and support are essential.

4.4 Key findings of the data analysis

- 96.25% (719) of the sample 2 participants do not have *any knowledge at all* of Blockchain technology or only *basics.*
- In sample 2, the overall trust level in blockchain to secure heath data is superior to ¾ (73.63%), representing 550 users. Americans are the most convinced with 91% trust in the technology. Europeans follow with 72% trust.
- Nevertheless, the research highlighted the relationship between knowledge of blockchain and trust in the technology. It shows that even though some of respondents do *not have any knowledge* of blockchain at all, around 70% of them trust it. The ones who have only basic knowledge trust it even more (86.99%) while Professional skilled people in the field really trust this solution to secure health data (90.91%).
- 66.18% (45) of the participants to sample 1 declared using at least one mobile application or any other connected object designed to track habits or medical condition. Tracking health habits is the primary reason for adoption of Bowhead Health (79,39%). The secured aspect of blockchain technology, does not to have a place at the core of the purchase decision of the patients yet (5.24%).
- 195 persons (26.1%) out of the 747 total respondents are patients suffering from a particular disease. Asthma (17.95%), Diabetes (8.72%), Heart disease (4.62%), Hypertension (13.33%) and Obesity (38.97%) being the most represented health issues. Hence, patients represent more than ¼ of the total users of the app.
- People surveyed on the mobile app tend to think that their data is safer (Secured at 54.62%) while a majority of participants to the online survey think their data is Vulnerable (50%).
- Conducted surveys reveal that patients are convinced and mostly in favour of the application of digital technology in health care, since it could spare stress, save time and energy.
- However, human contact remains irreplaceable, especially in the treatment of severe disease like cancer.
- There is a real need for transparency and privacy since health data could easily stigmatize people based on their health disorders

- Misuse or theft by third parties is a redundant concern, especially regarding insurance companies.

- Patients are open to give health data for research in their disease area, even if it means giving up on some of their personal health data

- An emphasis was made on the lack of communication between health organizations and mismanagement of data. This resulted in a numerous medical errors or assumptions affecting the patient’s care, especially for chronic disease.

- Patients are conscious that data can never be 100% secured but overall, blockchain technology convinces patients as it provides anonymization and transparency.

5. Discussion and recommendations

When combining the findings, the analysis of the surveys' data and the common themes in the interviews, it can be concluded that blockchain could help the adoption of digital health technology by patients, since it provides an answer to many of the raised concerns.

With the recent increase of companies offering telehealth solutions during the coronavirus, experts confirmed the many system vulnerabilities of these new eHealth solutions and their absence of proper standards, due sometimes to their label as wellness companies (regulations like GDPR do not apply the same way to a company with a wellness purpose than to a company with clinical health purpose) and to the lack of adapted legal framework and guidelines. As raised by Bowhead's CEO, it is the giants Google and Apple that "*had to prevent any developer from just launching a COVID-19 app. They only allowed apps that have some sponsorship or association with a public health agency or a research organization".* The collection and processing of personal health data must be carried out with respect for the patient's privacy, medical secrecy, and regulations in force. Unfortunately, not data could be gathered on the legal side, so this implies further research.

<u>Blockchain and Smart Contracts provide informed consent,</u>

It has been covered that Blockchain alone is not sufficient but is a good lever. This technology cannot store personal heath data as It would not comply with the GDPR right to be forgotten. It should then be associated with the use of smart contracts to be valuable in healthcare. The data confirmed the need to use smart contracts as it responds to patients needs of privacy by establishing informed consents. Meaning that the users is then fully aware of the use made from his health data. As a result, blockchain provides transparency and thus trust in eHealth.

Nevertheless, the research highlighted the relationship between knowledge of blockchain and trust in the technology. It shows that even though some of respondents do *not have any knowledge* of blockchain at all, around 70% of them trust it. The ones who have only basic knowledge trust it even more (86.99%) while Professional skilled people in the field really trust this solution to secure health data (90.91%).

As per the interviews, hypothesis would be that there is an elasticity relationship between patients' propension to share their health data and the rarity of their disease since they all mention they would agree to share their health data for clinical trials, even it would mean giving up on some of their health data privacy. However, for now it has been seen that 26.1% of the 747 total respondents are patients suffering from a particular disease. Asthma (17.95%), Diabetes (8.72%), Heart disease (4.62%), Hypertension (13.33%) and Obesity

(38.97%) being the most represented health issues. Hence, patients represent more than ¼ of the total users of the app.

In addition, the gap of injustice (insurance, employability, anonymity, etc.) that these data could incur if not protected covered in the literature, was confirmed by the interviews of patients fearing to be stigmatized as sick persons, even for contracts such as insurance coverage.s

5.1 Recommendations

Create a user data control dashboard

Like Bowhead's dashboard for researchers to access anonymized data, developing built-in dashboards for patients to access the inventory of the health data shared, historic of consents given as well as which organizations or HCPs received their data and what for is important. This way, transparency and privacy are not only promised, but displayed. Also, it has been seen through literature that integrating a visual representation or dashboard designed in a user-centred design (UCD) manner would increase value for the patients. The presentation of listed consents and data flows should be delivered in an ergonomic and simple design, minimizing the steps to access.

Develop a security indicator, a “blockchain-certified icon”

It has been seen through interviews and data analysis that people tend to trust a technology even though they do not understand the entire technical characteristics behind it. Moreover, reinsuring users of their data privacy was proven imperative.

This approach is similar to the identity button of a website that displays a padlock in the address bar of our browsers to certify that a secured HTTPS connexion is established with the website reached. In some circumstances, you may see a grey padlock with a yellow warning triangle or a grey padlock with a red stripe, alerting you that something is wrong with the website. Integrating the same visual tool in eHealth, especially mHealth, would accelerate patients’ adoption in the sense that it would ensure them that their transactions of health data are secured, because information such as the identity of a clinical lab for example, has first been cross-checked by blockchain technology.

If necessary, an information panel could allow the patient to view more detailed information about the security status of connection.

Simplify the general public's understanding of distributed ledger technology systems

During the research it has been shown that the majority of the samples' population had very little knowledge of eHealth and blockchain technology and its related advantages. Thus, rising patient awareness and potential interest on these matters would be a strategic move to increase patient adoption. Democratizing DLT throughout advertising, conferences, videos on social media to educate younger generations in having good security assessment reflexes.

Develop more partnerships with healthcare incumbents

Additional data would be required on the interoperability possibilities of blockchain between the incumbents, also a standardization of the health data exchange format is necessary for a complete compatibility.

On a second time, create a sense of community in the health technologies

Thus, allowing users to exchange and connect with patients that suffer from the same potential health disorders, answering to the need of guidance and support raised in the interviews of the patients. Bowhead Health implemented it this year and testified of a great retention rate.

6. Conclusion and further research

This paper has first explored the general context of the health sector and literature on eHealth expansion and its challenges with regards to big data and privacy. A focused literature review was conducted, showing the evolving relationship between eHealth and distributed ledger systems like blockchain.

Based on the literature and empirical work carried out, there are several ways in which blockchain is able to accelerate the adoption of eHealth solutions by patients for them to take back control of their private health data.

Indeed, the research has been able to show that most people surveyed needed reassurance on the privacy and security of their health data, which blockchain is able to provide.

Nevertheless, the research highlighted that a relationship between knowledge of blockchain and trust in the technology exists. Even though some of respondents do *not have any knowledge* of blockchain at all, around 70% of them trust it.

Moreover, the research showed that blockchain combination with smart contracts technology can revolutionize adoption since it answers to patient privacy, transparency and control needs. By simplifying users' understanding and ability to assess DLT by developing blockchain security indicators, facilitating the informed consent with user data flow control interfaces, as well as developing more partnerships with healthcare incumbents.

By creating technologies with such features, health actors foster the healthy development of a digital healthcare system that respects patients' needs and rights, especially privacy.

Finally, this paper adds to knowledge in the sense that it shows the benefits of blockchain in the patients' adoption of eHealth, by providing related insights on patients' perceptions, pain points, and concerns.

6.1 Directions for further research

This work serves as a humble contribution to the resources on implementation and workflows of blockchain integration in eHealth, for actors across the health care industry to understand patients' perspective in the process. The future implementation of DLT in eHealth will rely on continued analysis of best practices, patients' pain points, and potential solutions to mitigate existing challenges.

It implies that further statistical research can study the subject on a bigger sample and compare the findings with the current report. Also, it could be very valuable to undertake the calculation of sample 2 (in-app survey) confidence limits to ensure its complete reliability. As data continue to flow from the in-app survey, it could be noteworthy to compare the actual results with the future reports coming in to see if time has an effect on the adoption metrics, trust level of blockchain and health data safety.

The first survey sample did not cover enough of answers to reflect the mindset of the population as a whole. Hence, studying blockchain for clinical trials could provide valuable information and guidelines for start-ups and big actors of the field. Plus, the results could differ from those observed in this report.

This research was partly led during the COVID-19 crisis and there is a strong likelihood that health actors have reassessed certain of their capabilities during this period to better ensure health data safety. However, directions for future research include:

- Would big companies in the healthcare sector be ready to undertake such innovative projects including blockchain, often in collaboration with smaller entities like start-ups? Such advances require a change of approach for multinational actors like pharmaceutical companies and national health organizations. If some are open to innovation and the implementation of DLT, the giants of the health industry will first have to be able to communicate and actively promote change internally with their teams to shake things up, before trying to deliver better patient outcomes and convince the outside world at a big scale.
- Are distributed ledgers really the future of data security? Will distributed ledgers last? It has been highlighted by experts that Blockchain in healthcare could as well not be the ultimate future due to its immature state. In addition, encryptions schemes are volatile, "*if you encrypt data today, you want to make sure that you can re encrypt them afterwards*" warned Pierre-Mikael Legris. As for every technology, the trend could pass. Considering the fast pace at which technologies are moving, with the advent of quantic computers for instance, it can as well become obsolete in 10 years. We live in an area where two revolutions at the same time are possible.
- More incentives and investment should be made from governments to establish proper legal frameworks

7. Personal statement

On a separate note and in addition to the knowledge I have had the opportunity to absorb on health, digital health and blockchain technology, I would like to reflect on the lessons I have learnt throughout the entire process of writing this paper.

First, I realized that eHealth is really an interest of mine. Indeed, combining the power of digital technology to health systems for better outcomes has captivated me.

In terms of process, the definition and scope of the project took way longer than expected. Also, the more I went through the literature and analysis, the more I could see myself craving to include additional facts and figures yet very interesting, but not relevant to the thesis. Indeed, not getting lost in all of this information was a big challenge, especially in such a rich and complex sector like healthcare.

Lesson one: stay focus and in-line with the main question.

Then, coming to interviews, I had to refine my approach to patients in an ethical and transparent way that made them feel safe and comfortable sharing their story.

Furthermore, I have learnt a lot on business relationships, processes and confidentiality throughout the process and particularly in the different collaborations I tried to undertake. Managing external parties and actors to the project were challenging and could rapidly compromise the plan if not handled rigorously and in a continuous way.

Lesson two is: change is the constant, especially in the business world.

Time management was definitely a big piece of the work. I have tried to plan every possible outcome and unexpected event beforehand. However, COVID-19 was not foreseen.

On a final note, lesson three is: manage time carefully, stay calm and always have a plan.

Bibliography

AGBO, Cornelius C., MAHMOUD, Qusay H. and EKLUND, J. Mikael, 2019. Blockchain Technology in Healthcare: A Systematic Review. *Healthcare* [online]. 4 April 2019. Vol. 7, no. 2. [Viewed 12 August 2020]. DOI 10.3390/healthcare7020056. Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6627742/

ALLESSIE, David, PIGNATELLI, Francesco, SOBOLEWSKI, Maciej, VACCARI, Lorenzino, EUROPEAN COMMISSION and JOINT RESEARCH CENTRE, 2019. *Blockchain for digital government: an assessment of pioneering implementations in public services.* [online]. [Viewed 14 December 2019]. ISBN 978-92-76-00581-0. Available from: http://publications.europa.eu/publication/manifestation_identifier/PUB_KJNA29677ENN

BATRA, Sonal, BAKER, Ross A, WANG, Tao, FORMA, Felicia, DIBIASI, Faith and PETERS-STRICKLAND, Timothy, 2017. Digital health technology for use in patients with serious mental illness: a systematic review of the literature. *Medical Devices (Auckland, N.Z.)* [online]. 4 October 2017. Vol. 10, p. 237–251. [Viewed 20 August 2020]. DOI 10.2147/MDER.S144158. Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5633292/

BERN, eHealth Suisse, 3003, [no date]. eHealth Suisse. [online]. [Viewed 20 August 2020]. Available from: https://www.e-health-suisse.ch/fr/page-daccueil.html

Better World Campaign, March 2020 Presentation, 2020. [online]. Morning Consult, Better World Campaign. [Viewed 1 July 2020]. Available from: https://betterworldcampaign.org/wp-content/uploads/2020/03/International-Cooperation-Poll-March-2020.pdf

BHATTARAI, Priyanka and PHILLIPS, Jane L., 2017. The role of digital health technologies in management of pain in older people: An integrative review. *Archives of Gerontology and Geriatrics* [online]. 1 January 2017. Vol. 68, p. 14–24. [Viewed 20 August 2020]. DOI 10.1016/j.archger.2016.08.008. Available from: http://www.sciencedirect.com/science/article/pii/S0167494316301522

BIESDORF, Stefan and NIEDERMANN, Florian, 2014. Healthcare's digital future. *McKinsey & Company* [online]. 2014. [Viewed 11 December 2019]. Available from: https://www.mckinsey.com/industries/healthcare-systems-and-services/our-insights/healthcares-digital-future

BOBÉE, Floriane, 2019. Smart Contract : Qu'est-ce qu'un contrat intelligent ? • BitConseil. *BitConseil* [online]. 3 July 2019. [Viewed 12 June 2020]. Available from: https://bitconseil.fr/smart-contract-contrat-intelligent/

BOULOS, Maged N. Kamel, BREWER, Ann C., KARIMKHANI, Chante, BULLER, David B. and DELLAVALLE, Robert P., 2014. Mobile medical and health apps: state of the art, concerns, regulatory control and certification. *Online Journal of Public Health Informatics* [online]. 5 February 2014. [Viewed 15 December 2019]. Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3959919/

Bowhead Health - https://bowheadhealth.com/, [no date]. *Bowhead Health - Optimize Your Health* [online]. [Viewed 11 December 2019]. Available from: https://bowheadhealth.com/

Bowhead Health Whitepaper - The Future of Digital Health, For a Happier and Healthier World, 2017. [online]. Bowhead Health. [Viewed 4 April 2020]. Available from: https://www.gwkjbc.com/Uploads/2018-09-20/5ba351b959fbf.pdf

BROGAN, James, BASKARAN, Immanuel and RAMACHANDRAN, Navin, 2018. Authenticating Health Activity Data Using Distributed Ledger Technologies. *Computational and Structural Biotechnology Journal* [online]. 1 January 2018. Vol. 16, p. 257–266. [Viewed 20 August 2020]. DOI 10.1016/j.csbj.2018.06.004. Available from: http://www.sciencedirect.com/science/article/pii/S2001037018300345

CNIL, 2018. Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data | CNIL. [online]. 11 June 2018. [Viewed 20 August 2020]. Available from: https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data

COMTESSE, XAVIER, 2017. *Santé 4.0 : Le tsunami du numérique*. georg. ISBN 978-2-8257-1065-4.

Coronavirus disease (COVID-19) Situation Report – 190 - 31st July 2020, [no date]. [online]. [Viewed 1 August 2020]. Available from: https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200731-covid-19-sitrep-193.pdf?sfvrsn=42a0221d_4

DEL RÍO CARRAL, M., SCHWEIZER, A., PAPON, A. and SANTIAGO-DELEFOSSE, M., 2019. Les objets connectés et applications de santé : étude exploratoire des perceptions, usages (ou non) et contextes d'usage. *Pratiques Psychologiques* [online]. 1 March 2019. Vol. 25, no. 1, p. 1–16. [Viewed 20 August 2020]. DOI 10.1016/j.prps.2018.05.001. Available from: http://www.sciencedirect.com/science/article/pii/S1269176318300245

DICOM_JOCELYNE.M, 2020. Objets connectés et applications mobiles en santé. *Ministère des Solidarités et de la Santé* [online]. 13 August 2020. [Viewed 13 July 2020]. Available from: https://solidarites-sante.gouv.fr/systeme-de-sante-et-medico-social/e-sante/article/objets-connectes-et-applications-mobiles-en-sante

Digital Health Market Share Trends 2020-2026 Growth Report, 2020. *Global Market Insights, Inc.* [online]. [Viewed 7 August 2020]. Available from: https://www.gminsights.com/industry-analysis/digital-health-market

Distributed Ledger Technology Systems, [no date]. *Cambridge Judge Business School* [online]. [Viewed 12 July 2020]. Available from: https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/distributed-ledger-technology-systems/

EDUCATION, Kamalika is passionate to write about Analytics driving technological change, 2020. Use Cases that Explain Big Data and Blockchain Interdependence. *Analytics Insight* [online]. 2 August 2020. [Viewed 20 August 2020]. Available from: https://www.analyticsinsight.net/use-cases-that-explain-big-data-and-blockchain-interdependence/

Education: From disruption to recovery, 2020. *UNESCO* [online]. [Viewed 6 June 2020]. Available from: https://en.unesco.org/covid19/educationresponse

End of year data breach report 2019, 2020. [online]. Identity Theft Resource Center. Available from: https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf

E-santé: augmentons la dose!, 2020. [online]. Institut Montaigne. [Viewed 6 June 2020]. Available from: https://www.institutmontaigne.org/ressources/pdfs/publications/e-sante-augmentons-la-dose-rapport.pdf

EUROPEAN PATIENTS FORUM, 2016. *EPF Position Paper on eHealth* [online]. European Patients Forum. [Viewed 15 June 2020]. Available from: https://www.eu-patient.eu/globalassets/policy/ehealth/epf-final-position-paper-on-ehealth_19december2016.pdf

FRANKENFIELD, Jake, 2018. Distributed Ledger Technology. *Investopedia* [online]. January 2018. [Viewed 15 August 2020]. Available from: https://www.investopedia.com/terms/d/distributed-ledger-technology-dlt.asp

Fuite de données concernant le service de prise de rendez-vous Doctolib | Accompagnement Cybersécurité des Structures de Santé, [no date]. [online]. [Viewed 12 May 2020]. Available from: https://www.cyberveille-sante.gouv.fr/index.php/cyberveille-sante/1965-fuite-de-donnees-concernant-le-service-de-prise-de-rendez-vous-doctolib-2020

General Data Protection Regulation (GDPR) – Official Legal Text, 2016. *General Data Protection Regulation (GDPR)* [online]. [Viewed 20 August 2020]. Available from: https://gdpr-info.eu/

GUNDLAPALLI, A. V., JAULENT, M.-C. and ZHAO, D., 2018. *MEDINFO 2017: Precision Healthcare Through Informatics: Proceedings of the 16th World Congress on Medical and Health Informatics*. IOS Press. ISBN 978-1-61499-830-3.

HARDIN, Lauran and MASON, Diana J., 2020. Lessons From Complex Care in a COVID-19 World. *JAMA Health Forum* [online]. 1 July 2020. Vol. 1, no. 7, p. e200908–e200908. [Viewed 30 July 2020]. DOI 10.1001/jamahealthforum.2020.0908. Available from: https://jamanetwork.com/channels/health-forum/fullarticle/2768610

HESSE, Bradford W. and SHNEIDERMAN, Ben, 2007. eHealth Research from the User's Perspective. *American Journal of Preventive Medicine* [online]. 1 May 2007. Vol. 32, no. 5, Supplement, p. S97–S103. [Viewed 20 August 2020]. DOI 10.1016/j.amepre.2007.01.019. Available from: http://www.sciencedirect.com/science/article/pii/S0749379707000487

Home Healthcare Market Size, Growth Report, 2020-2027, 2020. [online]. [Viewed 7 June 2020]. Available from: https://www.grandviewresearch.com/industry-analysis/home-healthcare-industry

Home Healthcare Market Size Worth $515.6 Billion By 2027, [no date]. [online]. [Viewed 6 June 2020]. Available from: https://www.grandviewresearch.com/press-release/global-home-healthcare-market

How Blockchain Will Revolutionize Healthcare, [no date]. *Cointelegraph* [online]. [Viewed 30 July 2020]. Available from: https://cointelegraph.com/news/how-blockchain-will-revolutionize-healthcare

HUYGENS, Martine, 2017. 978 94 6159 780 9: *A patient perspective on eHealth in primary care: critical reflections on the implementation and use of online care services.* [online]. Maastricht: CAPRHI Care and Public Health Research Institute. [Viewed 6 January 2020]. Available from: https://www.nivel.nl/sites/default/files/bestanden/Proefschrift_Huygens_Martine.pdf

Industry leaders in blockchain technology worldwide 2018, [no date]. *Statista Research Department* [online]. [Viewed 20 August 2020]. Available from: https://www.statista.com/statistics/920747/worldwide-blockchain-technology-development-leading-industries/

Institute for Health Metrics and Evaluation - Global Spending on Health., 2016. *Institute for Health Metrics and Evaluation* [online]. [Viewed 13 December 2019]. Available from: http://www.healthdata.org/news-release/global-spending-health-expected-increase-1828-trillion-worldwide-2040-many-countries

ISLAM, Md Saiful, HASAN, Md Mahmudul, WANG, Xiaoyi, GERMACK, Hayley D. and NOOR-E-ALAM, Md, 2018. A Systematic Review on Healthcare Analytics: Application and Theoretical Perspective of Data Mining. *Healthcare* [online]. 23 May 2018. Vol. 6, no. 2. [Viewed 20 August 2020]. DOI 10.3390/healthcare6020054. Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6023432/

La fiabilité et la diffusion des informations de santé mises à l'épreuve par le coronavirus au Japon, 2020. *nippon.com* [online]. [Viewed 1 August 2020]. Available from: https://www.nippon.com/fr/in-depth/d00551/

LARS, Ludovic, 2018. Quelles différences entre blockchain publique et blockchain privée ? *Cryptoast* [online]. 20 June 2018. [Viewed 12 August 2020]. Available from: https://cryptoast.fr/differences-blockchain-publique-blockchain-privee/

LATULIPPE, Karine, HAMEL, Christine and GIROUX, Dominique, 2017. Social Health Inequalities and eHealth: A Literature Review With Qualitative Synthesis of Theoretical and Empirical Studies. *Journal of Medical Internet Research*. 27 2017. Vol. 19, no. 4, p. e136. DOI 10.2196/jmir.6731.

L'émergence du web 3.0 : L'Identité Décentralisée, 2019. *TheCoinTribune* [online]. [Viewed 12 May 2020]. Available from: https://www.thecointribune.com/analyses/lemergence-du-web-30-lidentite-decentralisee/

LI, Yan, BAI, Changxin and REDDY, Chandan K., 2016. A distributed ensemble approach for mining healthcare data under privacy constraints. *Information Sciences* [online]. 10 February 2016. Vol. 330, p. 245–259. [Viewed 20 August 2020]. DOI 10.1016/j.ins.2015.10.011. Available from: http://www.sciencedirect.com/science/article/pii/S0020025515007288

L'observatoire de la santé du futur, 2018. [online]. Paris: Viavoice Paris. [Viewed 6 February 2020]. Available from: http://www.institut-viavoice.com/wp-content/uploads/2018/12/Observatoire-de-la-sant%C3%A9-du-futur.-Etude-Viavoice-pour-le-groupe-Vyv.pdf

«L'OMS ne sortira pas indemne de cette pandémie», 2020. *Le Temps* [online]. [Viewed 18 March 2020]. Available from: https://www.letemps.ch/monde/loms-ne-sortira-indemne-cette-pandemie

LTD, Research and Markets, [no date]. Global Digital Health Outlook, 2020 - Research and Markets. [online]. [Viewed 7 May 2020]. Available from: https://www.researchandmarkets.com/reports/4833137/global-digital-health-outlook-2020

MARSCHANG, SASCHA, 2014. *Health inequalities and eHealth* [online]. eHealth forum, Athens: eHealth Stakeholder group, European Commission. Available from: http://www.ehealth2014.org/wp-content/uploads/2014/06/Pres_Marschang.pdf

MEHTA, Nishita and PANDIT, Anil, 2018. Concurrence of big data analytics and healthcare: A systematic review. *International Journal of Medical Informatics* [online]. 1 June 2018. Vol. 114, p. 57–65. [Viewed 20 August 2020]. DOI 10.1016/j.ijmedinf.2018.03.013. Available from: http://www.sciencedirect.com/science/article/pii/S1386505618302466

MESKÓ, Bertalan, DROBNI, Zsófia, BÉNYEI, Éva, GERGELY, Bence and GYŐRFFY, Zsuzsanna, 2017. Digital health is a cultural transformation of traditional healthcare. *mHealth* [online]. 14 September 2017. Vol. 3. [Viewed 20 August 2020]. DOI 10.21037/mhealth.2017.08.07. Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5682364/

MIKULIC, Matej, [no date]. Willingess to wear health tracking technology U.S. 2018. *Statista* [online]. [Viewed 13 July 2020]. Available from: https://www.statista.com/statistics/829479/willingness-to-wear-health-tracking-technology-us-adults/

NEWSROOM, 2014. Commission publishes four reports of eHealth Stakeholder Group. *Shaping Europe's digital future - European Commission* [online]. 11 April 2014. [Viewed 15 August 2020]. Available from: https://ec.europa.eu/digital-single-market/en/news/commission-publishes-four-reports-ehealth-stakeholder-group

NODE | meaning in the Cambridge English Dictionary, [no date]. [online]. [Viewed 15 August 2020]. Available from: https://dictionary.cambridge.org/dictionary/english/node

OLARONKE, Iroju and OLUWASEUN, Ojerinde, 2016. Big data in healthcare: Prospects, challenges and resolutions. In: *2016 Future Technologies Conference (FTC)*. December 2016. p. 1152–1157.

ØLNES, Svein, UBACHT, Jolien and JANSSEN, Marijn, 2017. Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. *Government Information Quarterly* [online]. 1 September 2017. Vol. 34, no. 3, p. 355–364. [Viewed 20 August 2020]. DOI 10.1016/j.giq.2017.09.007. Available from: http://www.sciencedirect.com/science/article/pii/S0740624X17303155

OLOGEANU-TADDEI, Roxana and PARÉ, Guy, 2017. Technologies de l'information en santé : un regard innovant et pragmatique. *Systemes d'information management* [online]. 1 June 2017. Vol. Volume 22, no. 1, p. 3–8. [Viewed 12 August 2020]. Available from: https://www.cairn.info/revue-systemes-d-information-et-management-2017-1-page-3.htm?contenu=article

PETERSON, Carrie Beth, HAMILTON, Clayton and HASVOLD, Per, 2016. *From innovation to implementation: eHealth in the WHO European region*. Copenhagen, Denmark: WHO Regional Office for Europe. ISBN 978-92-890-5137-8. R858 .P485 2016

Privacy, Protection of Personal information and Protection Rights, [no date]. [online]. UNICEF. [Viewed 6 January 2020]. Children's rights and business in a Digital World. Available from: https://www.unicef.org/csr/files/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf

Projet de loi sur les données personnelles : 5 mesures clés, 2018. [online]. [Viewed 13 July 2020]. Available from: https://www.editions-legislatives.fr/actualite/projet-de-loi-sur-les-donnees-personnelles-5-mesures-cles

Q4 and Annual 2019 Digital Health (Healthcare IT) Funding and M&A Report, [no date]. *Mercom Capital Group* [online]. [Viewed 7 August 2020]. Available from:

https://mercomcapital.com/product/q4-annual-2019-digital-health-healthcare-it-funding-ma-report/

Qu'est-ce qu'un smart contract?, 2019. [online]. [Viewed 12 August 2020]. Available from: https://www.youtube.com/watch?v=vQTs7NmTDa8

RAUCHS, Michel, GLIDDEN, Andrew, GORDON, Brian, PIETERS, Gina C., RECANATINI, Martino, ROSTAND, François, VAGNEUR, Kathryn and ZHANG, Bryan Zheng, 2018. Distributed Ledger Technology Systems: A Conceptual Framework. *SSRN Electronic Journal* [online]. 2018. [Viewed 12 June 2020]. DOI 10.2139/ssrn.3230013. Available from: https://www.ssrn.com/abstract=3230013

Reassurance on privacy of contact-tracing app remains "crucial," 2020. *Digital Health* [online]. [Viewed 7 August 2020]. Available from: https://www.digitalhealth.net/2020/06/reassurance-on-privacy-of-contact-tracing-app-remains-crucial/

RENATA BRITO AND JOSEPH, [no date]. Spain's new wave of infections hits the young, middle-aged. *Washington Post* [online]. [Viewed 15 August 2020]. Available from: https://www.washingtonpost.com/world/europe/spains-new-wave-of-infections-hits-the-young-middle-aged/2020/08/03/1313e42a-d581-11ea-a788-2ce86ce81129_story.html

RIO CARRAL, Maria del, ROUX, Pauline, BRUCHEZ, Christine and SANTIAGO-DELEFOSSE, Marie, 2016. Beyond the Debate on Promises and Risks in Digital Health: Analysing the Psychological Function of Wearable Devices. *International Journal of Psychological Studies* [online]. 12 October 2016. Vol. 8, no. 4, p. 26. [Viewed 20 August 2020]. DOI 10.5539/ijps.v8n4p26. Available from: http://www.ccsenet.org/journal/index.php/ijps/article/view/62409

ROCK, Leslie, [no date]. The Paperless Patient: Electronic Records Gain Ground. . P. 2.

RS 816.1 Loi fédérale du 19 juin 2015 sur le dossier électronique du patient (LDEP), [no date]. [online]. [Viewed 1 August 2020]. Available from: https://www.admin.ch/opc/fr/classified-compilation/20111795/index.html

SAFI, Sabur, DANZER, Gerhard and SCHMAILZL, Kurt JG, 2019. Empirical Research on Acceptance of Digital Technologies in Medicine Among Patients and Healthy Users: Questionnaire Study. *JMIR Human Factors* [online]. 29 November 2019. Vol. 6, no. 4. [Viewed 20 August 2020]. DOI 10.2196/13472. Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6911230/

SALGADO, Tânia, TAVARES, Jorge and OLIVEIRA, Tiago, 2020. Drivers of Mobile Health Acceptance and Use From the Patient Perspective: Survey Study and Quantitative Model Development. *JMIR mHealth and uHealth* [online]. 2020. Vol. 8, no. 7, p. e17588. [Viewed 20 August 2020]. DOI 10.2196/17588. Available from: https://mhealth.jmir.org/2020/7/e17588/

SAMARANAYAKE, Eshan, 2020. Telehealth, Telemedicine, and Telecare Explained. *Medium* [online]. 10 June 2020. [Viewed 19 August 2020]. Available from: https://medium.com/any-writers/telehealth-telemedicine-and-telecare-explained-1739d20913ec

SIMPAO, Allan F., AHUMADA, Luis M., GÁLVEZ, Jorge A. and REHMAN, Mohamed A., 2014. A review of analytics and clinical informatics in health care. *Journal of Medical Systems*. April 2014. Vol. 38, no. 4, p. 45. DOI 10.1007/s10916-014-0045-x.

SLEVIN, Patrick, KESSIE, Threase, CULLEN, John, BUTLER, Marcus W., DONNELLY, Seamas C and CAULFIELD, Brian, 2019. A qualitative study of chronic obstructive pulmonary disease patient perceptions of the barriers and facilitators to adopting digital health technology. *Digital Health* [online]. 25 August 2019. Vol. 5. [Viewed 28 July 2020]. DOI 10.1177/2055207619871729. Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6710666/

SOPRASTERIA CONSULTING, 2019. ENQUETE EUROPEENNE SUR LA DIGITALISATION DU PARCOURS DE SANTE, Juin 2019, SopraSteria Consulting. [online]. June 2019. [Viewed 1 June 2020]. Available from: https://www.ipsos.com/sites/default/files/ct/news/documents/2019-06/ipsos_sopra_steria_digitalisation_des_parcours_de_soin.pdf

STATISTA RESEARCH DEPARTMENT, [no date]. Global market for blockchain technology 2018-2023. *Statista* [online]. [Viewed 14 December 2019]. Available from: https://www.statista.com/statistics/647231/worldwide-blockchain-technology-market-size/

STATISTA RESEARCH DEPARTMENT, 2016. Global digital health CAGR by major segment 2015-2020. *Statista* [online]. 2016. [Viewed 25 May 2020]. Available from: https://www.statista.com/statistics/387875/forecast-cagr-of-worldwide-digital-health-market-by-segment/

STROETMANN, Karl A, THIERRY, Jean-Pierre, STROETMANN, Veli N, EUROPEAN COMMISSION and DIRECTORATE-GENERAL FOR THE INFORMATION SOCIETY AND MEDIA, 2007. *EHealth for safety: impact of ICT on patient safety and risk management : eHealth for safety report.* Luxembourg: Publications Office. ISBN 978-92-79-06841-6.

Telehealth Programs, 2017. *Official web site of the U.S. Health Resources & Services Administration* [online]. [Viewed 20 August 2020]. Available from: https://www.hrsa.gov/rural-health/telehealth

The Top 12 Data Breaches of 2019, [no date]. [online]. [Viewed 2 June 2020]. Available from: https://www.securitymagazine.com/articles/91366-the-top-12-data-breaches-of-2019

THOMAS, J. Graham and BOND, Dale S., 2014. Review of Innovations in Digital Health Technology to Promote Weight Control. *Current Diabetes Reports* [online]. May 2014. Vol. 14, no. 5, p. 485. [Viewed 20 August 2020]. DOI 10.1007/s11892-014-0485-1. Available from: http://link.springer.com/10.1007/s11892-014-0485-1

TILL, Brian M, PETERS, Alexander W, AFSHAR, Salim and MEARA, John, 2017. From blockchain technology to global health equity: can cryptocurrencies finance universal health coverage? *BMJ Global Health* [online]. November 2017. Vol. 2, no. 4, p. e000570. [Viewed 21 August 2020]. DOI 10.1136/bmjgh-2017-000570. Available from: http://gh.bmj.com/lookup/doi/10.1136/bmjgh-2017-000570

UKTELEHEALTHCARE, 2017. What is Telehealth? | UKTelehealthcare - Telecare, Telehealth and TECS Hub. [online]. 6 July 2017. [Viewed 19 August 2020]. Available from: https://www.uktelehealthcare.com/what-is-telehealth/

Urgent health challenges for the next decade, [no date]. [online]. [Viewed 1 July 2020]. Available from: https://www.who.int/news-room/photo-story/photo-story-detail/urgent-health-challenges-for-the-next-decade

What is Ethereum?, [no date]. *ethereum.org* [online]. [Viewed 12 April 2020]. Available from: https://ethereum.org

What Is Privacy?, [no date]. *Privacy International* [online]. [Viewed 10 April 2020]. Available from: http://privacyinternational.org/explainer/56/what-privacy

Appendix 1: Online survey questions

Please note that data of the two surveys, in English and in French, were merged for the analysis.

EN: Study on your health data and digital health

This 2 minutes-long survey, of approximately 10 questions, is designed to understand :

- how you view your health data and how important it is to you;
- your thoughts on the protection of your health data;
- your knowledge of new digital health/health technologies;
- the extent to which you agree to disclose your health data and for what purposes.

1. **You identify as:**
   - A man
   - A woman
   - Gender neutral
2. **You are:**
   - Under 20 years old
   - Between 20 and 29 years old
   - Between 30 and 39 years old
   - Between 40 and 49 years old
   - Between 50 and 59 years old
   - 60 years old or more
3. **What is the highest level of education you have completed?**
   - Compulsory education
   - Post-secondary level (Apprenticeship/vocational training, Gymnasium/vocational matriculation, diplomas)
   - Bachelor or equivalent level
   - Master or equivalent level
   - Doctorat or equivalent level
4. **Do you use at least one mobile application or any other connected object designed to track your habits or medical condition (connected watches,**

mobile applications tracking your sports, diet, treatment, disease symptoms, etc.)? YES/NO

If you answered NO to the previous question, please do not answer question 4a.

4a. If YES, what "digital health" devices do you use the most?

- A mobile application on my smartphone
- A watch/other connected application-related device
- A computer/ webpage
- Other

4b. If NO, why don't you use these types of digital devices to track your habits/ health status?

- I have no use for it.
- I'd rather talk to my doctor.
- I find it dangerous, I'm afraid my data will leak or be hijacked.
- I didn't know it existed.
-

5. **In which ONE of these situations would you be more likely to use these e-health technologies?**

   - If they were recommended to me by health professionals
   - If I was paid to enter my data
   - If I had a chronic illness or serious health condition
   - If I wanted to follow my sports/weight/diet
   - If their reliability was confirmed by the State/competent experts
   - If the media talked about it more

6. **In general, how secure do you think your health data are?**

   - Not secured at all
   - Vulnerable
   - Protected
   - Fully secured

7. **Would you be in favor of integrating this "digital health" data into our health insurance contracts (data on physical activity, sleep, alcohol consumption, headaches, etc.)?**

- Yes
- No
- Neutral

8. **Do you think that the data stored on these devices could help scientists to better understand certain diseases and thus develop more effective drugs?**
    - Probably
    - Unlikely
    - Neutral

9. **Have you ever consulted a doctor remotely (teleconsultation) and/or ever used an artificial intelligence tool for diagnostic?** YES/NO

10. **If you have ever consulted remotely, were you satisfied?**
    - Not satisfied at all
    - Partially satisfied
    - Satisfied
    - Very satisfied

11. **How do you see our current traditional health care system evolving with respect to digital medicine? (Open question)**

12. **What knowledge do you have of Blockchain technology?**
    - None
    - Basic knowledge
    - Advanced knowledge -> *if selected access to specific questions on blockchain*
    - Professional knowledge -> *if selected access to specific questions on blockchain*

13. **In the future, do you think Blockchain technology will be used and accessible by most of the population?**
    - Yes
    - No
    - Maybe
    - Neutral

14. **Do you think the use of Blockchain technology can help secure health data on a large scale?**
    - Yes
    - No
    - Neutral

Online survey: comments and additional material

Question 11. How do you see our current traditional health care system evolving with respect to digital medicine? 44 answers

No evolution
Slow evolution
More Digital integration
Telemedecine focus

Covid-19 as a driver
Benefits and Innovation
Security/transparency
Risks and misuses

- None
- We will evolve towards more telemedicine as a gate keeper to accessing specialists.
- Hopefully a better integration of traditional and digital medicine, enhancing the strengths of both, leveraging the wealth of data in a safe, secure and private way
- I believe in telemedicine, but connecting with my GP or with HCP recommended by GP
- I foresee that healthcare professionals may more and more rely on automated diagnostic tool and prescriptions suggestion. The development of medical tracking used by HCP may allow them to share more easily their patients' records, if patients consent. It would help drug design and test with real-world evidence. I also foresee that instead of starting from the drug and find its indication, the ext generation medicine will start from individual patients and find the best drug for their condition.
- Accelerating now with Covid, especially telemedicine
- I expect it to become more digital and virtual
- More telemed / more collboration between insurances and apps
- Moving toward virtual consultation with the pandemic. I personally have not experience it.
- I think we're going to move away from proximity medicine to integrate more global, less personal data, with less personal diagnoses.
- The corona virus Crisis will give a big push towards digital health!
- There is a lot of things to work on, in order to change to digital.
- It is at a point where it does not take the user's side into account. Nevertheless, it is on the professiovinal side quite efficient

- definitely an evolution, COVID-19 is a big driver, telemedicine is growing significantly
- It seems like they are getting more Integrated as technology evolves
- Personalised data and feedback
- Diagnostic supported by AI
- Corona kickstarted the process
- I see it as two separated things. The current health care system has no link with digitalization yet.
- Slowly but surely
- Too slow & not enough transparent
- It is moving way too slow. I would like to be able to do more online consulting as well as having a fully transparent digital patient log with all my health data.
- I see the system struggling between the possible and likely advantages of it but not daring because of confidentiality issues
- Almost no developement
- I see it as two separated things. The current health care system has no link with digitalization yet.
- Slow
- *Virtual* checkups and exams
- I'm afraid that 1. the data will be used to discriminate people (you will pay much more if you have a chronic condition) 2. that the mutualization of risk will be reduced thus the responsability of pushing healthier lifestyles will be shifted towards individuals entirely, which will favor the well-educated/rich at the expense of the lower socio-economic casts. The silver lining here is that with more data, technically it will be possible to identify or even predict health issues and diseases better. This will require a large change in the health industry (doctors and companies alike) which in the best case will take 10-20 years to happen.

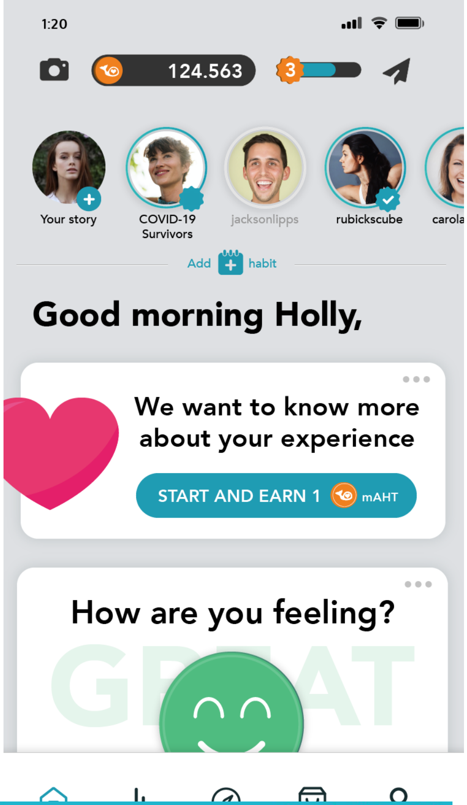
- Meilleur suivi
- Je n'en ai aucune idée...
- En suivant un système assez similaire au fameux "Big brother". De plus en plus de surveillance sur l'individu, contrôle de ses constantes et habitudes. Optique de partenariat commercial et possibilité d'effectuer une pression mentale sur la population.
- Vers le traçage de chaque individu et vers la stigmatisation des malades
- Que notre parcours médical sera rapidement visualisé quand on sera hospitalisé.
- Cela peut être très positif au développement mais comment être sûr des informations.
- Moins de contact humain, des diagnostics peu fiable, voir dangereux.

  - Se digitaliser de plus en plus
  - Dans le bon sens si la sécurité est garanti et la confiance suffisante
  - Vers une prise en charge encore plus efficace
  - Des abus arriveraient très vite pour duper ceux qui analyseront les données
  - Another big trend and need is interoperability of all the health care systems and data

- I’m not afraid to provide My health data in clinical studies or to my GP. I need to be protected by commertial initiative based on my health data as well as insurance company that can “limit” my or my family insurance coverage knowing health conditions.

- Coming for other continents, Europe is mora capable to switch to digital medicine than other places. Specially for their accessibility to health care.

Appendix 2: In-App survey in Bowhead Health Inc. mobile app



1:20

124.563

3

Your story

COVID-19 Survivors

jacksonlipps

rubickscube

carola

Add habit

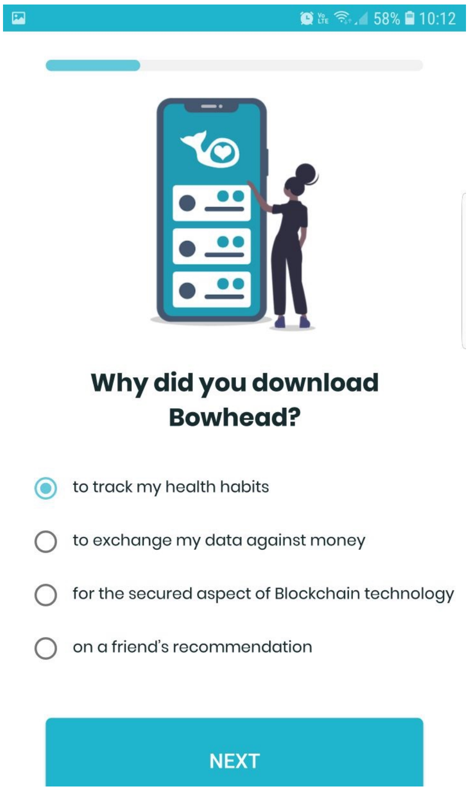
Good morning Holly,

We want to know more about your experience

START AND EARN 1 mAHT

How are you feeling?

GREAT



58% 10:12

Why did you download Bowhead?

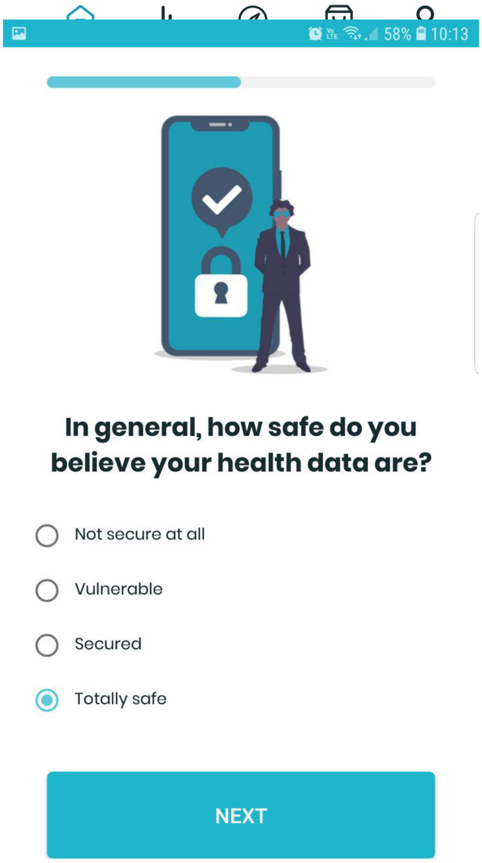
● to track my health habits

○ to exchange my data against money

○ for the secured aspect of Blockchain technology

○ on a friend's recommendation

NEXT



58% 10:13

In general, how safe do you believe your health data are?

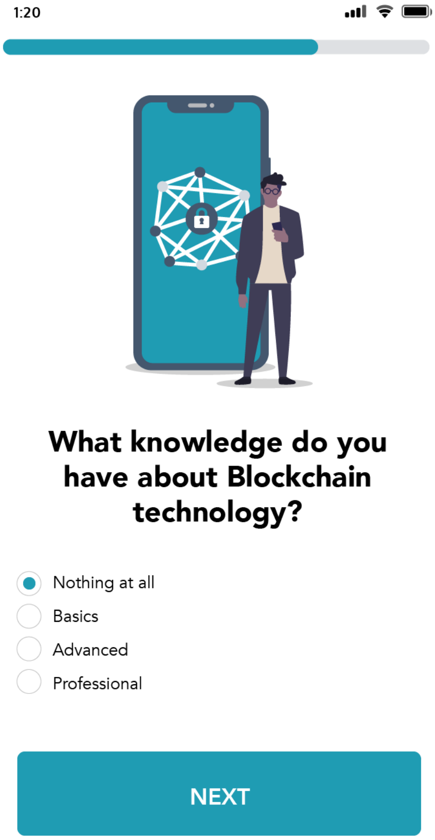
○ Not secure at all

○ Vulnerable

○ Secured

● Totally safe

NEXT



1:20

What knowledge do you have about Blockchain technology?

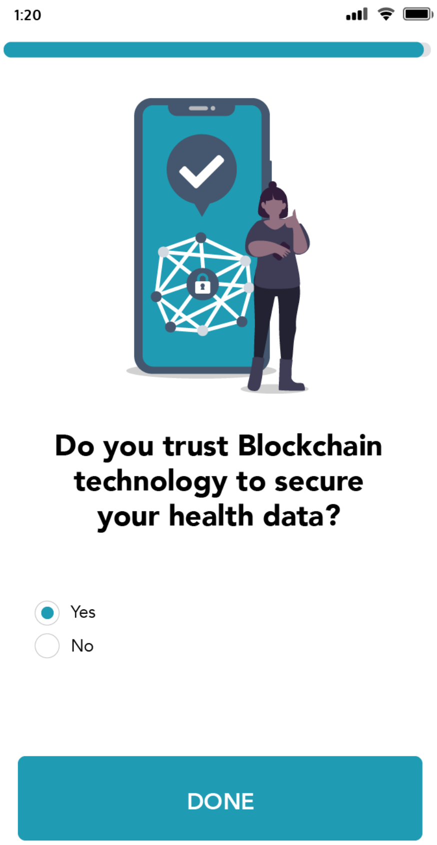
● Nothing at all

○ Basics

○ Advanced

○ Professional

NEXT



Do you trust Blockchain technology to secure your health data?

● Yes
○ No

For more information, please visit Bowhead Health website : https://bowheadhealth.com/

Appendix 3: Excerpts from qualitative interviews with professionals

Interview 1: Francisco Diaz-f Jr., CEO and co-founder of Bowhead Health

Date: 4th August 2020

Camille Rattazi: Do you believe in blockchain for the future?

Francisco Diaz-Mitoma Jr.: Yes, at Bowhead we believe that blockchain and specifically distributed ledger technology can enforce health data privacy, and secure ownership for patient data.

Camille Rattazi: Is our data really safer with blockchain?

Francisco Diaz-Mitoma Jr.: Our data is one step in the right direction with blockchain. There are many components that make up safety between a user, a client device such as a smartphone, and internet service providers, servers and the cloud. There are a lot of hops of data. We really need to focus on every single point on the data chain to ensure that it is using the right kinds of encryption, and that the data that travels is encrypted, and is stored encrypted with only the private keys that people control themselves. I guess the main point there is that, you know, blockchain is one component to help with that. But if we're talking about having our data safe, I think there's many different components that need to be considered.

Camille Rattazi: What could be those components, for example?

Francisco Diaz-Mitoma Jr.: For example, your smartphone, your Wi Fi router, the internet service provider, the actual server the way that it's configured to make sure that it's not accessible to third parties, which we've seen many cases where people are able to access people's private data. I mean, in Canada, for example, there was a company called Lifelabs that had a lot of patients. Data genomic records stolen from servers. So there's many different components that I think make our data safe. Blockchain can help with some of those components.

Camille Rattazi: I've discovered that in the United States, there are way more leakages than in Europe. In your opinion, is it only because of the difference of regulations?

Francisco Diaz-Mitoma Jr.: I think it also has to do with the number of private providers that there is. There's a lot more different private clinics, private hospitals, there's a lot of startups that are working with health data and sensitive data there, which results in a lot more kind *of points of failure. Within the health data infrastructure in the United States than in Europe, where a lot of the health data is managed by a country as a single kind of health care system, reducing the number of organizations that have access to sensitive health data and the number of risk*

Camille Rattazi: Okay, and in if you had to say, what are the main advantages of this technology?

Francisco Diaz-Mitoma Jr.: So the main advantage of blockchain is that it's a transparent system, where you may be able to see on the distributed ledger all the different transactions or events. For example, execution of a smart contract, or for example, patient providing consent to join a clinical study or for example, a patient Providing consent for their doctor to see their data. And everything becomes auditable on a distributed ledger.

Camille Rattazi: And the opposite what are the main concerns in your opinion?

Francisco Diaz-Mitoma Jr.: So the main concern with blockchain is that it's not easy to use. But I think that this is more of a task for user experience designers and developers. I've also heard many people say that the main concern is that blockchain isn't needed that a database can accomplish the same goals as a sorry that a blockchain can accomplish the same goals as a traditional database. But this hasn't been the case in the past and it won't be the case in the future, unless we begin using blockchain and distributed ledger technology. And I also think that as a society better understanding how our data is being managed, will also help alleviate some of these concerns.

Camille Rattazi: And terms of are we getting to the society in the future? Do you believe this technology will be? Even if it's complicated to use? Do you think there is a chance that it will be using and accessible by most of the population?

Francisco Diaz-Mitoma Jr.: Yes, I think the benefits outweigh the drawbacks of blockchain. And I think that there are policy changes occurring. And there's a lot of focus on health data privacy and security, which will force people to begin considering blockchain as the solution.

Camille Rattazi: do you think the digital health technologies could be developed faster, thanks to blockchain?

Francisco Diaz-Mitoma Jr.: Yes, when people feel their data secure, or if they choose to share de identified data, and only that consented de-itendified data is shared. They feel more comfortable contributing their data and this drives innovation of tomorrow. The flip side of that is if people don't trust technology or they don't trust, how their data is being *stored, then innovation and medical research becomes much more difficult and expensive because there's not as much data.*

Camille Rattazi: Okay, and do you think there are some people that will tend to share their health data based on their situation, for example, severe illness, or do you think that could influence the way they show Their data?

Francisco Diaz-Mitoma Jr.: Yes, I think that people with chronic illnesses or illnesses that aren't very well understood, have a vested interest in driving innovation for their own reasons. And they're willing to, to kind of share more data.. I don't have any data to support that. But it makes sense.

Camille Rattazi: Perfect. So here is a picture, so I'd like to know if this view of the society and the health industry is something that you think is possible ?

Francisco Diaz-Mitoma Jr.: Yes, I think this is a great diagram. I think that's kind of the future vision is to have all these key stakeholders that are listed here, for example, private companies, universities, hospitals, patients, doctors, insurance companies, contract research organizations, pharmaceutical companies, and the FDA. I think those are all key stakeholders who will be integrating or collaborating with this blockchain ecosystem. The one more component that you've mentioned here, which is validators, auditors and key keepers. I think that is almost another diagram where that is citizens.

But I think there's also this concept of democratizing even where the health data is stored. So one of the things that we've been exploring or thinking about dreaming about is, how can we further decentralize this network? For example, the way that Bitcoin and ethereum work where you have miners, where you have people that are dedicating their computer resources, whether that's bandwidth or storage, or computational power to act as validators, I think that people also can play an important role in further decentralizing this system and that's when the true power of blockchain comes into effect.

Camille Rattazi: It can be difficult in a blockchain to provide the right to be forgotten, which is in the regulation. What do you think of it? How do you deal with it?

Francisco Diaz-Mitoma Jr.: There's no health data stored on the actual blockchain. Only the encryption and decryption keys are stored on the blockchain. So there is a smart contract that we work with, that basically allows users to delete all of their health data that's associated with their account. And that, that takes care of kind of deletes. The second point to that is, for example, in GDPR, a lot of the concerns around a right to be forgotten, do not apply in the same ways for clinical research. So for clinical studies, if if you're part of a study *and you're getting paid for your health data or you're contributing your health data. The GDPR regulation is different. So I think there's two different separate streams of thought there.*

Camille Rattazi: Okay. But if we if we refer to the previous picture. We see that blockchain would be applied to validate all the data in this data driven economy. And but you're saying here that it does not it does apply only for clinical studies. So will the deletion of data work in this entire data driven system?

Francisco Diaz-Mitoma Jr.: Well, the deletion of data is technically possible because It's not stored on the blockchain. So if a user wants to delete their account and all of their kind of health data associated to it, they can they can, they can do that using smart contracts. Oftentimes, people think that health data is stored on the actual blockchain, but that's not the case.

That's right. So, for example, in our case, we use a storage file system called IPFS, which stands for interplanetary file system. And that is where the encrypted data is stored. So for example, if we have a campaign in United Arab Emirates, we will have a server physically in that country, so that we comply with data residency laws. If we have a camp is a study in South Korea, we will have physically a server in South Korea. And that is where the encrypted data is stored. If somebody would like to delete their health data, they're able to do that. Because that data is not stored on the on the blockchain.

Camille Rattazi: So now we move on to the more personal thoughts section. How secure do you think our health data are in general?

Francisco Diaz-Mitoma Jr.: I think this question really depends on where you live, I think in the United States Health Data is not very secure. I think that, you know, health data reports are still sent via email and in unsecure ways. I think there's companies like 23andme, who are these genomic companies that are being portrayed as kind of wellness companies that don't necessarily need to comply or hold personal health data to the same standards as they should. And then I think there's countries for example, like Estonia, where, or Finland that use a platform called x road, and it's a secure blockchain based system. I think that is a secure system. So I really think it depends on where you live in the world and which system you're interacting with. In regards to how Secure health data is but I think in general, are healthy, it is not secure. And that's just a way of life right now is that, you know, our, our banking details are more secure than our health data details.

Camille Rattazi: I could see that in Europe, as per the survey conducted online, people generally think they're held data secured, or only vulnerable. So obviously,

there are a lot of a lot of patterns and explanation to this. But do you think the government has a lot to play in this in this part?

Francisco Diaz-Mitoma Jr.: Yes, I think the the enforcement of health data standards is driven by the government in Europe. So I think that's probably Why, you know, people, people in Europe, when they think of their health data, they may think their health status is very secure, versus in other parts of the world, where, you know, there's a lot of different companies, for example, Apple, Google, that are trying to get more into the health data space. And I think that consumers in the United States, seeing companies like 23andme, and seeing these genomics companies who have health data leaks, I think the perception of how beta security starts to degrade.

Camille Rattazi: Is Canada during doing something in that direction, getting the government to kind of unify everything?

Francisco Diaz-Mitoma Jr.: Well, so Canada is an interesting example because it has you know, it has a healthcare system where any Canadian has access to healthcare. So there is kind of a unified body there. But it also allows for private companies that maybe don't have the best standards, for example, lifelabs. I'll use the example again, they had a health data leak, and millions of Canadians, genomic records were exposed. And I don't think the handling of that was appropriate. For example, now lifelabs is now trying to block the government from even releasing their findings on an investigation as to how that leak happened and who was involved. So I think that begins to also degrade users trust, at least speaking for myself, a Canadian, I think that reading reports like that doesn't make me feel good about my health data.

[…] they didn't follow the laws on kind of a data leak, and how to inform customers. But from what I've read, there hasn't been any large repercussion, which is a pretty big concern.

Camille Rattazi: So in in general, do you think that the sanitary crisis, helped to shift people minds towards new technologies?

Francisco Diaz-Mitoma Jr.: Yes, I think it's been helpful for people to understand the power of some of these large tech organizations, for example, Apple and Google working together on this Bluetooth contact tracing solution. I think that really kind of showed the world that, you know, technology can help us in certain situations. And these larger organizations are willing to work together to accomplish population health goals. But I think that it also puts a big spotlight on health data privacy. I know a lot of people that have said, I'm not going to install that because it's going to be tracking me or I, you know, it also has led to a lot of confusion because there's so many new technologies. There's so many new apps that, for *example, Google and Apple had to prevent any developer from just launching a COVID-19 app. They only allowed apps that have some sponsorship or association with a public health agency or a research organization. So I think it's helped people kind of shift their minds towards new technologies. But it's also created a lot of confusion for people because there are so many new technologies available.*

Camille Rattazi: is there still work to do regarding how people trust that technology?

Francisco Diaz-Mitoma Jr.: That's one of the big concerns is - trusting this COVID-19 pandemic is over - What happens to all of that data? Who's owning that data, who's managing that data? Who's accountable for that data? These kinds of questions that are unanswered. And this would be good on a policy perspective of kind of having some guidelines of saying if you're collecting Data during the pandemic for health data, you must follow these steps and I read that in Europe, they were beginning to discuss that.

But it would be a good thing to look up to see if there was any resolution passed, because there were some pretty important framework there where if you were a private company collecting health data, you had to delete it after the pandemic or after a certain amount of time. So I think these are the things to consider and look at kind of the best examples and problem with the law is that it is often a few steps behind. They cannot follow good technology or they're having a hard time following with regulations. Policy is a little bit slower to implement than technology.

Camille Rattazi: So in general, do you think patients will be open to the digitalization of the healthcare system?

Francisco Diaz-Mitoma Jr.: It's linked with trust and privacy. So I think people and patients are open to it. I think, to some extent, more than the word open. I think that they're being forced and pushed ainto the digitization of a healthcare system. And we can see this around the world, right. The number of people that were going into emergency rooms or the number of people that were doing elective surgeries actually drastically dropped during COVID-19. Which means that you have kind of this accelerated rise of telehealth, which is obviously, digital, digitizing records digitizing the experience. But also, there's an increased security risk because of this move to telehealth. Now you have, again, a lot of companies that have popped up over the last few months that are offering telehealth solutions, maybe have certain system vulnerabilities. So I think that we need to be cautious about having the right framework security policy in place to make sure that people's health data is protected during this process, because it's no doubt that it's going to happen are all our electronic medical health records are going into that direction and this accessibility through telehealth and *even, for example, with a zoom call. So, it is important to keep top of mind security just so that it's going to help the progression to digitization.*

Camille Rattazi: It has definitely helped with the telehealth adoption. But do you think this trend is going to last or do you think if we come back to a totally normal life, people will totally stop doing telemedicine?

Francisco Diaz-Mitoma Jr.: I think that telehealth is here to stay. Because it's just much more convenient as well. And there's a lot of people who live in rural places that don't have access to hospital. There are some people that live an hour away from their closest hospital. So, now if you have the convenience of telehealth might be the first kind of touch point that you have instead of driving to the hospital for an hour, you can click a button and have speak to a doctor.

Camille Rattazi: So, now I have some results about the study I have already conducted. The majority of the participants do not have any knowledge at all or only basic knowledge. of blockchain technology. What do you think of this? And how should we act to accelerate this adoption?

Francisco Diaz-Mitoma Jr. : So I think that is very surprising. It's a higher number than I thought. […]I definitely think that there's a lot of room for improvement in the way that we explain blockchain or we explain our how security works, so that people but are more cautious about how they use different products as it relates to their health data. So, the answer is yes, I think that we should accelerate the adoption by having mini tutorials in the app as well as articles and hopefully we can even show your thesis.

Camille Rattazi: I was very surprised because I tried to link trust with the knowledge of blockchain. So, out of the persons that declared trusting blockchain, the majority of them do not have any knowledge of it at all. And I think that says a lot, but what are your thoughts on this?

Francisco Diaz-Mitoma Jr.: Again, I was very surprised by this. And I think that it has a lot of this a lot of similarities with, for example, banks, right. So, do you trust where you're to trust the bank? Do you trust that the money that you have in your account is safe there when you go to sleep? I have a feeling that a lot of people would answer yes. Although they don't really understand how the banking system necessarily works. Or another example might be if you send money to somebody across the globe to another country, and you trust that service. For example, these digital money sending services you might not know how it works, but you'd trust that it will get there. That might be a similar kind of perspective here where somebody might not understand the underlying technology, but that they trust it *simply because they've heard of it or they've seen it being used by other large corporations or they've seen the impact it's had in the financial technology space where people have digital wallets, for example, virtual currencies, and they trust those wallets that hold those currencies. So, I think that people can trust the technology without necessarily understanding how it's used. But I think that one of our main goals is to educate people on how the technology works and helping them become literate on health data security.*

Interview 2: Pierre-Mikael Legris, CEO and co-founder of Pryv

Date: 14th July 2020

P-M. Legris: I am a software engineer by training. And I have always been, I would say in entrepreneur mode, in the sense that even before the end of my graduation at the EPFL, I was already part of a startup. And I have never left this environment since then. At some point 15 years ago, I spent about eight years extremely sick between my home and the hospital. When you're a patient, chronic patients actually don't like hospitals, you try to escape from them. And when as I am a software engineer, one of the ways for me was to collect as many data as I was able to and to provide to my doctors, and the data was okay if your temperature raise over these for more than one hour then you call us and come back. So at some point I was spending all my time sick so I started to track other information about myself. So, not only health data that were required by the doctors, but also my life data beat like what quantified self-person can do when they measure themselves. Like even number of steps, my sleep time or whatsoever, and trying to find correlations between my life, the medication and my conditions.

P-M. Legris: […] And typically what I noticed and was able to show to my doctors, is that my work time were predicting my white cells counts, which was pretty important for them. And why because actually, I was working less before.(…), for me, the trigger was to count my work time to as the best match I could have to see if I need to take more or less medication. But then if you start doing that, and if you want to reproduce it for others, then you want you understand that you want to really the intimate life of persons. So it's not about just doing something for myself on an Excel spreadsheet or stuff like this. If you want to industrialize such product, you have to be extremely concerned by the privacy of persons.

Camille Rattazi : And did that bring you where you are now in your company?

P-M. Legris : Exactly. And the thing is that privacy we took it on a totally different angle than what usually people do. Usually people understand privacy and it's a very important part is the security part, which usually translate in the digital world by encryption. We use encryption technology but not on our system not on pryv company product. We use third party technology we don't develop our own encryption methodology or since they use what we developed is a way to mobilize the data so people can understand it. At Pryv we do not have patient data, we sell the software to store these data.

So I mean, people can understand the data and decide who has access to what, and change his mind at any point of time. So they say I share some data with my General practician

(GP) I want to change my data, I can remove things and I can also check when the doctor had access to my data.

Camille Rattazi : Could you explain to me what's behind the technology they are using for you?

P-M. Legris : Why we do not use encryption? Why would we do not use encryption ourselves for a simple reason is that the life of encryption scheme is quite short. An encryption scheme today, no one will tell you in five days, in five years, it will still be the standard of encryption. So it means that if you encrypt data today, you want to make sure that you can re encrypt them afterwards. Okay, and this is why we didn't take the path of having our own technology, but better to use the technology of others, where it's their job to always provide the best technology ever.

Our job is really to be at the top of the content management. The question we want to make sure that our I'm the one that use our software can answer is if someone comes to them and say, Can you tell me which data you are you of me? Can you tell me with which consents you collected this data? Can you tell me who had access to what, when and what for? And I want to change this and eventually I want to erase or a part of my data. Which we can do.

Camille Rattazi : Did you consider blockchain or not at all?

P-M. Legris : We did consider blockchain and when it was because we started in 2012. So we considered blockchain from the start from day zero. And there is a problem with blockchain that cannot be solved, if given to you that if you use a blockchain to store medical data, there is very nice usage and we do use blockchain. (..) if data is just stored on the blockchain it means that this data is going to be spread around on multiple nodes that obviously no one fully controlled because this is the concept of the blockchain is that there is several tenants several parties that holds the blockchain right? If you put personal data it means that you have to encrypt them.

Okay. And as we have mentioned before, an encryption methodology does not last long. So if you put your medical records on a blockchain it means that it has been spread around to multiple tenants and that they even have the time to try to crack it down and to find about your data and there is no way no way that you can erase your data in the blockchain. Okay, so that's domain for you. Not even for me, it's also for the regulation is that if you have to comply to the GDPR, or to the CCPA in California, and to the right to be forgotten, no one can, blockchain cannot provide this right to be forgotten. Some people will tell you just have to throw away the keys. But you know that the data is there.

Camille Rattazi : And that's not the case with your technology, you can you can erase everything ?

P-M. Legris : Our technology is standard. It is a standard database. So then it has to be encrypted to be protected, but then come back to standard encryption. Okay, even if we use and we are investigating some stuff that are proxy encryptions that really allows fine grained control. But at least you control who has the copy of your data because we do not prevent if I send you a copy of my files - You can still keep a copy of the files. That would be illegal but you still can do it. While in a blockchain even if I tell someone and say oh by the way this user requested to erase the data, no one can come and erase part of the blockchain because then the blockchain becomes invalid by design. So, where we did use a blockchain and we developed even our own. It's actually for transaction logs. So instead of storing the data, we stored proof that the data existed on pryv. Okay, and proofs that a constant was given. For this a blockchain in healthcare is really powerful. Because what you can do is, for example, I share data with you and you can check that the data you received is really mine on a blockchain because I can put on the blockchain a signature of the data I sent to you.

Camille Rattazi: Plus, it's useful because you always want to keep approvals and consents. You don't want to erase it right?

P-M. Legris: Yes, for the consent, it's obvious in smart contract, but more for clinical trial. Let's say that you do an investigation on a new medicine. But actually, at some point, you find out that this medicine is not working, you might be tempted to modify the results. Okay, but if you put a checksum of all the transactions for this clinical study, then it means that if someone touches the database, you cannot find back what was the result but you can prove that the database has been modified, and that the clinical trial is invalid.

[the following text were translated from French]

Another use is, when there are several parties involved. One of our clients has to share data with an external party, for example an hospital platform, a blockchain could be great, with smart contracts. Since they can prove they received the consent from a certain person to share the data on both platforms.

That's where the blockchain is interesting, in the link or the evidence. On the other hand, for storage, if someone tells you that they are storing patient data on a blockchain, they will not be compliant. Unless they've come up with an incredible way to delete the data from the blockchain, but in essence that's impossible.

You very quickly find yourself in systems where you lose control for data protection reasons. It works very well in the financial framework, the blockchain keeps all the transactions made by a wallet and as long as the owner of the wallet is unknown, everything is fine. However, if one day we find out that it's yours, that becomes serious.

Storing personal data does not work in a blockchain.

Camille Rattazi: What if we do not collect personal data like names or email in the first place?

It could work, but you never know if the next data that will be added to the system won't be the one that can identify you. Very often if these data can be put together, the owner can be recognized. It requires effort, but still. We realize that what can betray is not only the name or the email, a geolocation, but the fact that there is, for example, only one man in the canton of Uri who has taken a certain medication. It takes very little to find out who a person is.

Camille Rattazi: So if there is a way to find the person, it is not consistent with the GDPR?

Sometimes the data is too important not to be shared. For example, data on cancers in Switzerland are, by law, shared. This is a public good. Some northern countries also do it, as soon as drugs are reimbursed, the data are put in a common pot.

Anonymisation is a finite means, but never guaranteed. Informed consent is king. If a person agrees to give his or her data and understands what is at stake, there is virtually no stopping it in any country. That is why smart contracts should be put forward, in a blockchain it's great. I have no doubts on the subject. They make it possible to verify that this contract was made today.

We are always going to find limits, but it's like an invoice, you can't go and ask a company to delete an invoice for your purchase. It needs it as part of its business.

What is essential is that people understand the exchange that is being made. If so, that is not a problem.

Camille Rattazi: Do you think people will be open to the digitalization of the health sector with technologies like blockchain? Or at least open to understand?

To be honest, understanding the blockchain is very difficult even for us engineers, it takes a lot of thought and time to assimilate it. You can't ask people to fully understand it.

I think it will be similar to the trust we have in banks. For example, we trust our bank, but we don't trust it because they're super good, we trust it because they send us a statement every month of what happened to our account. We wouldn't trust a bank that would only give us the final balance of our account without any further explanation.

The world works a lot like that today, there are very few companies that send you reports on what they have collected on you. I think this will be the first development. The first ones that will stand out from the crowd by doing this well, will become trusted databases and companies. Also, I think the blockchain will be useful for the identification of people, especially in medical processes.

The general public will not think blockchain. They will trust the actors responsible for using it to ensure security.

I don't believe too much in decentralization. Companies will be trusted to establish secure technologies among themselves. This will not involve showing patients data sequences. It comes back to the little locks in web browsers URL, personally I see the padlock and therefore I trust the site. You see it, so you know it's secure. Same with door locks, you trust the locksmith, but you don't fully understand the mechanism inside the lock. We're in that phase now, in terms of digital technology.

I believe exposing technology is a proof of weakness. If we trusted the blockchain in itself, which is a technology, if there was a problem, who we would turn against? Someone has to be responsible.

[…]

Interview 3: Alexis Roussel, COO Nym Technologies SA

Camille Rattazi: Thank you So much for accepting this interview and for your time. So, Mr. Roussell, could you please introduce yourself?

Alexis Roussel: I'm a lawyer specialize in new technologies. And I worked for seven years in the UN as a government officer specializing in helping cities to implement government projects. And then I moved to the private sector, especially the crypto finance industry where I created financial broker of cryptocurrency broker. For that I that I run for six for six years. And now I joined a company which is called Nym, where I'm the COO of this company in charge of all the operations and its companies building a privacy and network That is run through blockchain.

Camille Rattazi: What would you say is the ultimate goal of your company?

The goal of Nym is to provide a network where all the metadata is being removed. So, there is no you can transfer any data from one person to another without any possibility that a, an analysis and anonymization is made. So, the idea is that really to provide the very strong resistant privacy network,

Camille Rattazi: Do you have examples of collaborations, if you're allowed to say, which kind of companies do you work with?

Alexis Roussel: Okay, so for now we are on an early stage because we are developing the network and the network is running only in the test net right now. So there is no official application yet. But what we're looking at is, for example, applications like messaging, where a service provider like signal, for example, who is a messaging app, would be able to relay all the messages from all the users without having zero knowledge of the of the users itself without having the IP address without knowing where those people are located, by also protecting against timing attacks. So there's a bunch of attacks which are possible when you Just looking at the Internet and how data is transferred. And basically we're trying to hide most of these data to, to confuse anyone who would be watching the network. And so the idea is that you can really run a privacy friendly messaging system, for example, where the not not even the the service provider or any person who would be observing the network, like a state. It wouldn't be possible for them to identify individuals who are using the domestic immune system.

Camille Rattazi: Could your network be applied to every sector or do you focus on a specific sector ?

Alexis Roussel: it is agnostic. Any data can go through it through it. So it's more network. It's a network layer element. So any kind of data can go through. And just to give you an example, there was some discussion at one point that for the COVID apps, their COVID tracing apps that were being developed, that the messages between the phone app, and the servers of the government would go through a mix that and because then it will, in reality, the current system is is not anonymous, its dominance. So you can always with some effort, trace who is connected to the server, and who's talking to the server and who's using the app. And so by using a mix that then you can actually remove this connection.

Camille Rattazi: We're going to go back to it later on. But the COVID apps really raised some questions for the populations. I could see that a lot of people do not want to download it by fear of the tracking. Even if it is highly recommended by the government.

Do you believe in blockchain for in the long term?

Alexis Roussel: No, I don't believe in the blockchain. I believe in value in cryptocurrencies, in the values and interest in digital trust that we are building. And blockchain is just one of the tools which allow to build this. But blockchain itself is completely useless and has no future. What you're building with a blockchain and with cryptography and with open source technology and with a protocol and if you combine a lot of technologies together, you create crazy stuff like Bitcoin or like applications that can run on their own. But blockchain is off is in my head has no future.

Camille Rattazi: So you are saying there needs to be a different set of technologies with blockchain to implement a correct system.

Alexis Roussel: It's just a when we're talking about blockchain blockchain is a very specific piece of technology which is a subset of Bitcoin and other cryptocurrencies. And it is a subset which is useful for to create Bitcoin and to create Ethereum. And before that, it had no other use cases where we could use a blockchain there was no use cases except for a cryptocurrency. It created an environment when, where we see the advent of shared computing or public and transparent shared computing, where you can run an algorithm in a public way and they are not dependent on one specific server. They're running on several servers. There is the advent of internet computers have a new something which didn't exist blockchain today is part of this, but it tomorrow, maybe not. And the problem today is that blockchain is a word which is being used badly, too, because it's hype and it's cool. And, and, and it usually tries to avoid the discussion with the real thing, which is the value which is created there. So the advent of digital value, this is the future. Today digital value is built *with a blockchain. But tomorrow it might not need to have a blockchain might need to have something else. Actually the peer to peer network as well. More important than the blockchain itself.*

Camille Rattazi: I was saying, when you think about digital value, what exactly do you mean? Do you mean for example, consent and smart contracts?

Alexis Roussel: Exactly all of this. All of this if you have, a smart contract, which is just a little software, which is running, which is running on a peer to peer network. And it's and some of the data of it is stored in a blockchain. And to run this that this is software you need to actually make transactions of digital values like Bitcoin or like ether. So blockchain is only one small part of it which has in reality. Blockchain is not well understood right now and it's being used for something which is not. So what is important is the digital trust and shared computing of the future. And, that's why any project which is trying to match blockchain with another industry, and blockchain in house will fail. And, and one day, maybe there will be a health service that will be using part of a blockchain behind but it's not because they're using a blockchain that they will succeed is because they will understand how value is being transferred, and how trust is being managed. And that they will use that in the correct way for the user.

Camille Rattazi: Are our data safer with distributed ledger technology, especially blockchain?

Alexis Roussel: No, it's not. Because blockchain is just a public ledger and the public ledger as everything is public and once you once you can put something on the private ledger, you can never ever remove it on there. private ones are fantasy

Because again I come back on the on the original point what is important is the shared computing and the value that you create okay. And these systems are being built on opens on open systems. So, if you want to have you want to create a smart contract that everyone can use, then the smart contract has to reside has to live on a public network and sustained by a public blockchain. If one point there is a if the blockchain for example, is private, then become non trustworthy. and the value of the trust which isn't licensed there just disappears. So any any private blockchains will ever hold a trust because it's not verifiable. It's part of the being public, being open, being shared. So that Everyone can use it can have access to it can have a copy of it, of the blockchain and of the network and have everything, all the elements of the system. These are all crucial elements so that you create trust and security. And if you remove one, for example, if you say, oh, but this data is stored on a private blockchain, then you don't have any benefit of using a blockchain, you can, you should just use a normal database and most immune system like we've been using all the time. So when here when we're talking about blockchain, the only valid use case today of blockchain is inside a public, transparent open network.

Camille Rattazi: And this as you said, would not work for our healthcare system, it would fail?

Alexis Roussel: I mean, you can you can, it can work for healthcare systems, but it depends on the use case. As an independent today on the technology today, the only real case we want to the only case, which the block a blockchain system in large is capable of achieving today is proving it's proving transparently that the payment has been made from one person to another. Okay? So that's that's the, what we are capable of doing right now. And, and so, if a house system needs to prove that the payment has been done by one person to another publicly, then we can add then of course, this is a use case that can be used for for public services, health services, but today the when we talk about health data, health data they should not be today at the current state of affairs should not be on the public open network, because the problem of these public open networks sustained by block chains is Once you register, record data in there, then it becomes it stays there. It stays there for life. And you can encrypt it. Okay, that's fine. You can encrypt it. But one day, anything, which is anything that is encrypted can be decrypted at one point. And so the security in time is not guaranteed on the data that you would store on the blockchain. So no data, our data are not saved on a blockchain. Does a blockchain system can help in managing our data, our personal data? Yes, I do believe so. But that's not the question.

Camille Rattazi: Blockchain is often used just to store proofs of consents for example. And then if people want to erase their data they just go with the smart contract and erase everything.

Alexis Roussel: No, no, no, because you can always keep a copy of our things, that the whole if you're on ether is sharing the whole the whole blockchain and the state machine both you can keep copies of it and you can see how they evolve. And you can analyze this. So, you can see when the person is giving consent, and when a person is removing consent that you can you can in those system, but if the data of the health data itself is stored, or some elements of the health data stored directly in there, it is a problem. Because you would see that even if it's encrypted. When you create systems, it's very important to see what data do we put in the blockchain and what is not there.

Camille Rattazi: It is definitely something that is complimentary to other systems.

So do you think this these distributed ledger technologies could help the health industry and digital health in a way to develop faster. Do you think that's something?

Alexis Roussel: Yes. So, so everywhere where you need traceability. Okay, which means for example, and medical production, maybe medical shipment, drugs, drug production drug, you know, like the truck testings and the build processes, which need to be the public house, clinical trials, and things like this, where all those documents and information that needs to be traceable and public. As long as there is no personal data. Because the problem was medical data is that it requires a huge amount of data. When you talk about medical data, data, it's not just text, it's pictures scans, 3d prints 3d files, to represent any kind of part of the body. (…) . So these are specific type of encryption, where you can prove something without revealing it. And, and then you could share this, this data. But again, I don't think it would be more blockchain. It's more the collection of data that would work there. (…) the other the other part which could help is on the identity management. To identity there is a lot of work on self-sovereign identities and how to manage identities through a blockchain or a blockchain system as a whole. And that could be a way for health system to be managed instead of having a centralized system for the for the identity management now, I'm not talking about the data itself, because data it will be very hard as I said, is highly technical and very high volume data will be hard for people to manage to stick to the software all the time and themselves. So but the identity that is attached to this documents could be managed in a decentralized way. But so, so this is like all the identity project which already existing.

Camille Rattazi: When you say identity management, you mean being sure that for example, a Doctor is sending some papers to the patient, is the patient really the person who received it.

Alexis Roussel: For example, yes, I think that could be one example. That because of because of the cryptographic properties of the identity systems. Basically, when the doctor is sending something to the patient, he knows that this is exactly the same patient that has was presented to him with this with a digital signature and he doesn't need to, to prove anything more or it doesn't need to ask because the cryptography is here, really helping to but if that's not just that's not just for, for health, it will be the same for finance and for other services.

Camille Rattazi: I see and and in your opinion, what is the role of the government in all of this?

Alexis Roussel: the role of the government is to help produce standards. So, whenever you have systems that are extremely complex, and you have like zillions possibilities on how to implement them. And still there is a lot of uncertainty on how the system will look like based on your user experience based on how science is evolving because there's a lot of research going on going cryptography and we still have a lot of things to learn.

So although system and they will evolve very quickly, they are evolving very quickly and they and what the government can do is not trying to impose a system because that's a rare thing that happened, we can see, every time they were imposing a system, it was a failure usually. And, but it's about more about putting standards. So protocols, deciding which standard they're going to use to exchange data between hospitals, what kind of standard they're going to use to identify the patient, what standard they're going to use to store the data of the of the patients. And once they define the standard, they leave everyone implementing those standards. So basically, standards, and they have to choose the standards in a way, which they think is the most protective for the individual, protecting not just in terms of data, but protecting in terms of the autonomy of the person that's I think that's crucial, especially in your house, is that when you're thinking about protecting. The data currently, the government only thinks about protecting the data in the term of security in the term of for instance hacker or mean foreign state that wants to access my data, and I do need to protect it. That's what the current concept of security is. But the security shouldn't be in that sense it should be how do I make sure that the individuals whose data is there has his autonomy his way of his capacity of making personal choice based on his own information, this is secure. (…)

Camille Rattazi: This schema of a data-driven economy is actually the dream of a lot of people I interviewed, where actually people, key keepers have full knowledge and control of their data. And they are actually rewarded for generating new data. There are actually several companies and persons that aim to do this. And I would like to know if you think this is possible to implement it on a big scale, nationally?

Alexis Roussel: Of course, it's impossible. Why? Because the reality is the following Today in Switzerland, about 8% of the people don't have a phone, you know why? Because they are kids, because they're elderly people because they're in the middle of a hospital with the brains with a brain damage for example. Some people are incapable of having a connection and interaction with technology. And if you if you count all the people who are not self-sustained, you know, with in the end, they have to have a tutor. So a lot of people about 20 to 25% of the population is not capable of managing their own life currently, and for many good reasons, because some of them are just kids who are two years old. Okay. So system where you imagine all the population having an app and everything controlled by an app is nonsense because it doesn't include everyone. So that's the first thing that is important. So, the system that we will see will maybe use part of this maybe there will be a part of connections connectors like you described them there. (…)

So the system this graph here is doesn't contain the connection with real life and the part of real life that it will always have. That's what I see…

Camille Rattazi: How secure do you think, or health data are in general?

Alexis Roussel: Well, now it's not that bad. Actually. Not that bad. Except from time to time. There's a big database that gets hacked. But I mean, all the smaller databases, your doctor database, the small things there, they're quite okay. (…)

Interview 4 : Anonymous – Data Analytics Manager in the Health industry

Date: 3rd July 2020

Camille Rattazi: Could you please introduce yourself ?

Unknown Speaker: I'm currently working at XXX. And I'm in charge of analytics for the region. And as part of the broader scope of my role, which is mainly about privacy, customer data, I've been working a lot on also the digital transformation and focusing on the on house data, and especially how blockchain can play a role in making sure that data is of better quality is more secure and more ethical for patients.

Camille Rattazi: Do you really believe in in blockchain for the future?

Unknown Speaker: Really, so I fully realized that technology itself is still very unproven in many aspects. Certainly, there is more hype and, I truly believe that it is much better than any type of Central solutions that we have. So will it be perfect? Certainly not. But anyway, evolution and transformation is made one step after the other, and actually believe that it's, it's a next step worth exploring for, I would say, for individual goods, because the people as individual will have more control on their data, better quality, etc, but also as a societal good, because if we have access to more for equal long data, this would be really the moment where actually we can we can safely tap on the mass and the quality of data to to leverage AI or any type of future technologies that we'll need to run those algorithm to improve general care. So there is a macro and a micro element to it.

Camille Rattazi: In your in your opinion, are the data safer with blockchain?

Unknown Speaker: Yes, it should be safer. There's also I would say, and again, that's the fault between theory and practice. Because what we see at the time being so in theory, if we are purist on the way that blockchain is made, etc, yes, it should be safer until at least the moment when we start to have quantum computers that can handle the and actually decrypt the encryption. Now, with what we see today, there is no pure blockchain solution available and there is always a mix that is on chain and off chain. And of course, anytime there's a part that's off chain, there are some vulnerabilities but again, comparing to having older data centralized, you know, cloud actually believe that is essential.

Camille Rattazi: Do you know any other technologies that would have the properties of blockchain nowadays? That could help with the security of data management and security.

Unknown Speaker: I would say in general no. Then you can be semantic and whether you call it a blockchain, distributed ledger technologies, etc. But I would say the key point I believe is that, you know, the, to the data to be truly safe. There are three things to do. First of all, there needs to be a policy element to it. So there needs to be a clear statement that individuals are the sole and true owner of the data, then the data needs to be distributed, that means it's not located centrally, and then it needs to be encrypted.

Camille Rattazi: Do you think blockchain technology will be used and accessible by most of the people?

Unknown Speaker : Well, then it's first to be to be an intention to it. So, you first need to have regulatory companies, private public, that there needs to be at first some players that are actually working, working on that. So, that will be the first moment because you cannot make it accessible to people. You need the technology to be there to be coordinated. There is a need also to work on the interoperability. So that's also a key point. So either because there are several different type of blockchains that need to talk between themselves or especially more realistically in the short term, that for blockchains to talk with the with traditional systems. So those are adaptability, interoperability.

So social data needs to be the study's general. First, that needs to be a framework that makes it more or less user friendly for people to try to adopt it. But then there is also an element that's very important, and absolutely not, not a given is that you need two people to trust the technology to use it. And we see there were a couple of recent articles, an article from the 11th of March that's showing that the adoption of digital health tools is decreasing before because people are not trusting that their data is safe. So in theory, blockchains should be the solution. But if you go and you ask people about blockchain there is this tendency also to distrust experts. So even if you have a tech expert that is telling you that this is the best technology there will be people that will be screaming conspiracy theory etc so this is also something that will discredit the tech. the last part that's also to hurdle is that even for the people that know blockchain many people know blockchain as the tech behind the Bitcoin and many people also just think Bitcoin as you know the, the dark cryptocurrency.

Camille Rattazi: You talked about the experts, the tech experts, but do you think it will help if the medical experts were recommending those kind of blockchain technologies?

Unknown speaker: yes, to some extent, but there will be a huge issue. So I think that the credit crisis was very telling, there are people that just don't believe medical experts. So it *will not be the one the one ultimate solution I think that's something that we'll never be able to get to. But of course, the more endorsement the better it should be.*

Camille Rattazi: Do you think the coronavirus has helped to shift people's minds towards eHealth technologies?

Unknown Speaker: I think it helped if we can say for her for deadly disease, it helped at least put some light on this privacy focus. And especially on the heart of the debate, which is, if you want results with today's technology, if you want results, you innovate privacy, you saw that the countries that could go they weren't. That had a big impact by using technologies. They did it by actually having a huge breach of individual privacy. So and then that's it that's basically waiting the short term of public safety to the long term, the long term trust and an access to data and I cannot judge what is right or wrong data, but it's just a fact. In the traditional model to be successful, you need to be privacy. Innovative. So it at least it brought the discussion to the table. And I think that it might help for people to be more sensitized. (…)

Camille Rattazi: Maybe people got comfortable with video conferencing or eat consultation. I had one this morning with my doctor, which is something I would have never done if we weren't in a current state.

Unknown Speaker: So yeah, it shifted at least the habits of Zero constant. That's very true. That's really true and also, perhaps even more even before going to that, simply using alternative tools just be good for setting a checkup. Before we will I be taking the risk of going to a to a waiting room in a hospital or at a doctor. So I'm spending time to check etc, which can be, which can be good or dangerous, because so if you go and use Dr. Google as as your main source of authority, that there might be some risks. But again, it's a it's a balance, but it definitely it will drive some newer and different behaviors.

Camille Rattazi: And in terms of the healthcare system, how do you do you see our current traditional healthcare system evolving with respect to this Digital medicine?

Unknown Speaker: Well, good question I expected to change but I expect it also that there will still be some going back to some traditional hurdles. So, that would be back and forth that will be like, forced or breakthrough that will accelerate it, then there will be go back to tradition. I personally lived myself trying, you know, to go to the physician and showing my physician a log of symptoms that I used an app to log symptom when my condition was acute. So which is normally should be much better than telling him well, when I'm in front of you, my symptoms are mild. So, I don't recall but my physician totally dismissed it, and you didn't want to look at it. So, again, I'm just looking for one example and there will be some

Data expected to go in waves. And I think the most interesting part is basically the if you draw a line between those waves, is it taking up or being flat? I still believe it would be taking up. I would love to have a major resolution, but I would say that's my unfortunately from experience I haven't seen. I haven't seen those. Those radical revolutions are happening in a sustainable manner.

Camille Rattazi: Do you think blockchain could help DHT to develop faster?

Unknown Speaker: Yes, but not directly, because this is just an enabler, but it should help basically getting quality. And once you get data of quality and you get data into quantity, so basically you get quantity and quality. Then again, digital has specially the algorithmic part of digital has needs, you need to feed the system with data. So the more data, the better quality of inputs you will get. So if you get you create good experiences and good experiences being with patient and doctors, they will be more willing to use it so it will create a virtuous cycle. So I see it as an enabler and I would not pretend that blockchain is the reason but blockchain would be the engine in the background. And potentially what we would see is that we don't talk about blockchain anymore. This is the protocol to process data. It's like today when you go and you search for something online, those are just not the good protocol that we're working with and enabling the functionalities that we use today. So, so hopefully we get we get to that. And that will also take a bit of the heat from the philosophical discussion of the tech and actually most talking about what is the result and the health outcomes that we want to have.

Camille Rattazi: So do you think the patients and the people would be open to these major changes? What were the kind of feedbacks you got when discussing with digital healthcare professionals around you?

Unknown Speaker: What I see and that's again, not the point where I think that even because you know that usually you have early adopters, you have the mainstream and you have the laggards. And so, like everything, so you will have that. But the point that's interesting here and it comes back to my first my first aspect is that in that case, the early adopters are people that are tech savvy. And, and to likelihood that people that are tech savvy, actually are more attuned and sensitive to the, to the to the data privacy question, which prevents them actually to early adopt. This is higher. I can give you an example I I would even if I would pretend, I'm usually an early adopter. I was piloting some of those apps, etc. But a couple of things that as of today, I would never use I would not Never use any type of, of Homer DNA testing kit. I don't want my DNA data to be in a cloud somewhere. I don't control it. So, so even if I'm at an early adopter, you see that I have those hurdles. So basically, if you think of the adoption as a bell curve, if you want the curve to be as wide *as possible, you need to address the privacy part. But seeing that, now, even that has permitted donated the main domain core of the bell curve that has sort of privacy concern. This is if you allow me to say concerning because even if the early adopters aren't convinced, the other ones are impossible to reach afterwards..*

Appendix 4: Excerpts of qualitative surveys with patients

1. “Marc”

Interview in French not transcribed.

Main points were:

- Lack of communication between hospitals
- Constraint to reexplain the medical path and disease
- Waste of time and stress caused by going back and forth to the hospitals for small talks
- Privacy important but feeling that healthcare actors are totally overwhelmed by events
- Incapable of handling such amount of data
- Suggest that data should be centralize regionally at least

2. "Sophie"

Camille Rattazi: Thank you for your time. Sophie, could please introduce yourself and the goal of your company?

Sophie: Well, my, my name is Sophie and I'm {an active member} at ESCA Cancer Support. A non-profit association. We have professionals and volunteers who offer emotional support, practical health well-being activities to those affected by cancer. Our services are all in English. Our target population is mainly the international community in the Lake Geneva region, which is substantial. And we have been around for 20 years, when the need was really being recognized there were people being diagnosed with cancer, who worked in with the multinational or worked in one of the international organizations, therefore their French was not that good yet. (...) We have about 300 members. We offer, one to one counseling with professional counselors, mental health professionals, counselors and psychologists. We offer well-being activities such as yoga, and lattes and gym and these are taught by professionals who are specifically trained to work with cancer patients. We have support groups in one in Geneva and one in Luzon. We also have a special breast cancer group, so they meet and they also do other activities together. Because we found that probably 60% of our database was breast cancer related. So that's a very important group. And they have very specific issues and very personal issues. (...) We offer support and our services are free of charge. And, we feel it's just it's a very vital service that we provide to the local area.

Well, back before back before Coronavirus. We had a nice beautiful center that we just moved in on February (...) that's just open to the public. (...) there is a library of books and pamphlets and a variety of resource materials for people. And yet people can just drop in, talk to a volunteer, have a cup of coffee, have a cup of tea, and nine times out of 10, that's exactly what they were looking for. Someone else to talk to who had been in the same situation or knew where they were coming from. (...)

Camille Rattazi: We talked a lot about the Association, which I think is amazing, the work you do is tremendous. But I would like to know more about you. You mentioned you were a patient as well in the past?

Sophie: Yes, so I moved here from the US {years ago}, and about a year after moving here, I found out when my mother was diagnosed with breast cancer, and she had a very serious and a very advanced breast cancer, and within two years she had passed away. But it was *during that time that I found out that I had this huge family history that just wasn't talked about [..]. So I'm very grateful actually to the Swiss medical system because I told my gynecologist the story, and he said, Well. I want you to go see the genetics department at the HUG. (...) And then in 2002, I had an abnormal mammogram. So it was just on a routine mammogram, so little calcifications, but it turned out to be malignant, but it was very, very early stages. In fact, it was called a ductal cell carcinoma. [...] I was very lucky because I had been followed so closely. But I still had treatment decisions to make. (...) So my treatment options were to have essentially prophylactic bilateral mastectomy, because of the family history even though I did not have the mutation at that time or to have a lumpectomy and radiation and then start on the anti hormone medications such as tamoxifen. So after much online research, and that's when I discovered ESCA cancer support, I was trying to find someone who had to make the same decision. Or, or even close, and I couldn't find anything in 2002, it was actually quite difficult to find any support of any type. It's come a long way since then.*

Camille Rattazi: And doctors couldn't help with the decision?

Sophie: Well, doctors don't want to tell you what to do. They say, here are your options, and I appreciate that. But you still, sometimes you'd like a little bit of guidance. […] Because I found that for myself, it was very important to have that support just someone to listen to you or someone who knows where you're coming from. You can talk to your family, you can talk to your friends, but they don't understand. And after a while, they get tired. They don't wanna hear about it anymore. They just want to hear that you're fine, and everything's fine. (...) So it all went very, very well. I've had no problem since then. (...) I'm very happy with the decision I made back in 2002. So I've been very fortunate, and I have my checkups every every year. Everything's fine ever since.

Camille Rattazi: I'm glad to hear that thank you so much for sharing your story.

Camille Rattazi: In terms of medical appointments? What was your daily life like? Did you have a lot of medical appointments after being diagnosed?

Sophie: It was probably weekly with the mammogram, seeing the doctor, the biopsy, then there's a waiting period for the results, got the results. Then I had to go and talk to a plastic surgeon and a breast surgeon and an oncologist. So yeah, it was set weekly and sometimes more than once a week, for the appointments after the surgery. (...) Then they said everything is fine. You just need to have a checkup every year now.

It's at that point, people start to feel a bit lost. Because for some people, it's a year or more when they are completely engulfed in this medical world where they have appointments and *treatments and chemo and radiation and something all the time. But at the same time, they're feeling like someone's doing something. It's okay because they're fixing me. And then when it's over, a little bit of fear creeps in and anxiety because you think well hang on what what if it comes back before next year when I come see you. How will you know? How should I be seeing you more often? So that's where a little bit of anxiety comes in. And that was the same for me. Because I've realized that's where the support is very important. And that's where after those medical things are over, that's where the associations play a huge role. is it okay, if I go out and do this, or can I? Is it okay to go back to work? Am I going to do okay or how do I answer questions my colleagues asked me, so that's where the patient associations play the most important role is to get the person back reintegrated, both socially and professionally. (...)*

Camille Rattazi: Coming back to these appointments, do you think some of them could have been avoided?

Sophie: I think a bit of it could have been done digitally. If you'd asked me that last year, I'd have probably said no, but again Coronavirus and the world of Zoom now, we're all living virtually and if it saves a person a trip or stress, who knows how far they have to go to go to the doctor's office. Then I think it very well could be the way for the future. Why not have a digital appointment, because sometimes I did go in just for checkup and basic questions like : How are you feeling? Are you having any issues? Anything you want to talk about? And that was it. It was just a checkup, just to check and see how I was doing. So I think some could have been done online.

Camille Rattazi: I'd like to ask you about the security of your data privacy. Do you feel and did you feel at the time that your health data were secured? And how do you feel now?

Sophie: To be honest, I think I felt it was probably more secure back then. That maybe that's a false security feeling that I had, maybe ignorance of how it all works, but I do feel there could be definitely issues with security now. I think facilities and medical professionals do the best they can. Hopefully, at ESCA CancerSupport we're very conscious of privacy and data protection and I guess the one thing I was a little worried about, back in 2002, was again because I am from the US, US health system. It's good, but at that point of time was a little restrictive. There was this fear of if they find out. (...) when we looked into getting insurance in the US, and insurance for me, because I had a history of cancer was going to be astronomical. I know it's a fear in the US, as far as security, that the insurance companies are going to find out that you've been diagnosed with something or that you are even having *the genetic testing (...) then that's a pre-existing condition, and we're not going to cover you. So I think, just from my experience, that was the biggest security fear.*

Camille Rattazi: In terms of digital technologies, what do you think of it?

Sophie: I love digital technology. I think we're learning a lot in this age of COVID-19, of what can and can't be done digitally. All those services I told you in the beginning that ESCA Cancer Support offers, gym, yoga, support groups, counseling. We moved it all online. However, we do realize it's not ideal. Not Enough. It's not how we want to function. Right now where we cannot come together. It's better than nothing. But when there comes a time when we can open the center again, that's where the important exchanges happen. And the important support takes place. I think there is a a place for digital technology. There's more now because of COVID-19, the digital technology has advanced very quickly. And it's been opened up to many more people. So that even somebody like me, who would I would never have used Zoom. (...) Now I realized wow, it went very well using. But it lacks the human touch and human touch in the medical field, especially in the cancer area is so important. So I think there are areas where digital technology is perfectly placed and the more you can do the better. But then there are areas where they think that personal touch is still the most important thing. So why not combine the two?

Camille Rattazi: How would you feel about sharing your data on digital health technologies? For example, sharing that this part of your body hurt this week or what feelings you experienced. Would you be comfortable putting it on the app instead of telling it directly to your doctor?

Sophie: Yeah, I think so. I think there are a lot of people that would be comfortable doing it that way. However, I think I would be personally hesitant to put anything really personal on there. I think I would tend to use an app more for my information. You know, I'd be looking for something or I use Fitbit or I use the Samsung Health app. (...)

Camille Rattazi: Would you share you health data if you knew it could help research or clinical trials in cancer?

Sophie: Yes, I would.

Camille Rattazi: Do you think that the fact that you've suffered from a severe disease is influencing the fact you would agree to share more of your health data?

Sophie: Yes, I think so. I know that there are many people who are so skeptical of digital technology. And then they you know, we have some people who are, I don't want to use that app, I'll just give you a donation. So I think it's just maybe just in my personality that I *would like to help people. So if using my information can help professionals or scientists develop something or come up with an idea that can help someone else in the same situation then why not? I mean, I don't see a negative.*

Camille Rattazi: As long as you remain sure that your privacy is insured?

Sophie: Yes. I mean, as long as somebody doesn't have my bank details for example, I don't care. I mean, they know, I had breast cancer and I had DCIS, etc. It's not a big secret. I'm not that private person. I know. Some people are very private, (...) For me it just doesn't matter, if it helps somebody, why not? what's the downside?

Camille Rattazi: So you would agree to that as long as your insurance company do not have access to it, correct?

Sophie: I think that my only level of skepticism is insurance companies now, yes.

Camille Rattazi: Do you think these eHealth solutions would be more spread if there were recommended by doctors?

Sophie: Yes, probably. But I think we have to be careful. (...) There are people out there who don't have the best intentions at heart. And so these things, I think they all have to be very carefully monitored. Because I think people who are sick are vulnerable. And they could be hurt by someone who's trying to abuse them in some way. (..) So I think they're good, but I would feel that some doctors might be a little hesitant, depending upon what the app does. If you've got apps that is gonna have chat rooms, then someone has to be monitoring those to make sure that nothing untoward is going on, or improper informations not being fed to untrusthworthy people. For example, I've got the cure, you just have to send me $5,000 and I can cure you. Some people are vulnerable, and they want to believe those things.

Camille Rattazi: Do you think that having kind of a dashboard summary of who had access to what data could help people to trust more these new health technologies?

Sophie: Yeah, I think the more transparent it is, the better.

Camille Rattazi: Do you think COVID-19 made people change their opinion towards these technologies, especially the patients you work with?

Sophie: Oh, definitely. As you can imagine a majority of people who come to us for help are of a certain age, because the highest risk factor for cancer is age. So we have a lot of people who, who said, Oh, I don't know how to use this zoom thing. I'll never do that. Never. Now there's Zoom and they're zooming all over the place. So I think they, they appreciated it *more. And what we have found during the confinement and in this whole period, is that people actually needed support, way more than before, because all of a sudden, especially people that were in treatment, they could not even see their own families for their own good.*

3. “Anna”

Camille Rattazi: So could please introduce yourself and tell me more about you?

Anna: I'm English, born in England, but I came out here when I was just married because my husband had been moved out here and I worked here as a freelance and I couldn't have a full time job at first being a foreigner unless the rules were different when I first came up. […] So ever since then, I've been really a freelance still doing the same thing still writing or editing or using my English. I then had cancer 20 years ago and I decided to get into ESCA. And I felt I could be useful that as someone who'd been through cancer and so I did become very involved in ESCA not quite as an even as that see, but in my own way I was helping people who had cancer or going with them to doctors or whatever supporting them. I went through the training sessions there. And that's what I still do. I'm an old lady now, but I like to be active. (…)

Camille Rattazi: May I ask you what type of Cancer you had?

Anna: yes, I had colon cancer. And it was and my mother had died at the same thing […] I just went to have a colonoscopy. And there it was, I had tumors and I had no symptoms at all. So it was very lucky that they found this. And I had surgery. I had surgery twice, and then regime of chemotherapy. And since then I've been fine. But it was at the end of my not at the end of my treatment, but several years afterwards about 15 years afterwards. I was asked if I'd take part in a genetic testing, ethics study. So I did, because I thought if it's a genetic counselor, which it is sometimes considered to be, then it would be a good from the point of view of my children and grandchildren if they could use me as a study. So I did that about five years ago.[…]. I don't think that is something that could have been done by technology because I had to go every time and talk to them. I couldn't see why I had to actually go physically when they gave me the results.

Camille Rattazi: How often did you have to go there and talk to them?

Anna: Well, after the surgery, I would I then Had a course of chemotherapy which lasted for months and then I had to go once every three weeks.

Camille Rattazi: And you mentioned that for some part of the important moments technology could have helped? With transfer of informations?

Anna: I don't think things were so advanced then I really felt the need to talk to someone face to face. I really felt the need to go and have a long chat with the oncologist to know *and I think that was very important. One time later on when I was working with it, first, I was supporting a patient and I accompanied her to the hospital where she had to make a decision whether she was going to have chemotherapy or not. It was a young doctor. And I was a little bit put off by his attitude because he was looking at the screen the whole time. He never actually looked at her that rather put me off sometimes this, he was giving her the percentage of success in teaching people or treating people her age was already in a fairly advanced age[…] And so I was a bit put off by the fact that he was talking looking at the screen all the time and talking to her so this was her decision and she could never actually have a face to face conversation which I feel is terribly important when you're being given bad news.*

Anna: It's probably a generational thing. All the people, you know, are not quite so quick on using technology is the younger generation. But I do think also, the doctors are not very, very good at giving bad news. (...) sometimes they're not terribly well trained or they don't have the training given to them and not enough time is is spent teaching them how to deal with patients who are frightened and worried. (...)

Camille Rattazi: What perception do you have of digital health and the Do you trust this technologies?

Anna: Well, I've never really used it in regard to my health. And the only question I've dealt with a lot of questions concerning health insurance. And, obviously, confidentiality is terribly important when you have to deal with health insurance as well, because you don't necessarily want the insurance companies to know all your antecedents.That would be my my reservation. I know that the health insurance companies themselves Hell's employ doctors and to, you know, to give their opinion. So that could be a conflict of interest. At some point there, I think. That is that's the slight reservation I have about this. Sometimes, some of that could get out. Some of the information could get out. I don't know, maybe by mistake or whatever. But I think the security of health data is very important, but I don't actually have Anything tracking on on my devices that tracks my health.

Camille Rattazi: Do you trust the security of your health data that your doctor and the hospital has?

Anna: Do I have the choice? I'm in very good health now and I just see a general doctor general practitioner once a year just a blood test. But I know she knows everything because all my data is shared between everybody my general practitioner and specialist may have consulted, so I know that when I go to see my general doctor, she knows everything. About *me that's happened during the year. Yes. I guess that's a good thing. And I don't really worry about it. I can't see the point in worrying about it.*

Camille Rattazi: What if your doctor would recommend to you to use an application to track your vitals, would you do it?

Anna: I go to a family doctor in a village you know, it's not a big deal. It's not a big hospital or anything like that. (…) I've never had it proposed to me to do any of these things. I'm not sure how I would react. I can't quite see how it would apply to someone in my case.

Camille Rattazi: my point was to try to understand if potentially people who have cancer or chronic disease would want to share their data more. If, for example, you could help scientists develop medicines against cancer, would you?

Anna: I suppose, if one was asked to participate in a study, as I was asked to participate in this genetic study, for example, and I agreed, because I thought it could be helpful to other people, particularly my own family, of course, that said that I didn't really hesitate apart. And I suppose if an insurance company got hold of that data and notice that my children, it might affect my children's insurance if they knew that their mother had had a genetic disease. I suppose that might affect them. That would be the only slight worry I would have.

Camille Rattazi: Did you used telehealth during covid-19?

Anna: it didn't apply to me in that case, because at the moment, I'm in good health and I just go once a year.(...)

Camille Rattazi: So, to summarize the main point for you is to protect data from insurance companies and ensuring security and your privacy, obviously.

Anna: Yes, I think it's a very good thing that doctors share more information among themselves. Because in this in the past, often they didn't and you had to repeat all your, all your history and every time you went to a different doctor. (..) But I was lucky I had a good all-around doctor who looked at the patient as an all-around person. (…)

There is a lot of psychology in that, especially with cancer, you know, because it's a scary disease and to have an encouraging oncologist who knows and keeps up with all the latest developments as well.

Camille Rattazi: How do you see with all of your experience and help us? Oh, hell experience what do you see this industry evolving? How do you think it will be in 10 years?

Anna: I think probably people will use a lot more technology and that's true as in every part of life and probably will evolve like that. I can't quite see that you will ever replace the human aspect but it'll obviously perhaps relieve some of the medical profession of some of the basic stuff they could be helped with. And I think yes, one has to be very careful about sharing data and I don't know how, one can be sure that your data is not being tracked by somebody. I don't know how you can be absolutely sure about that. (…)